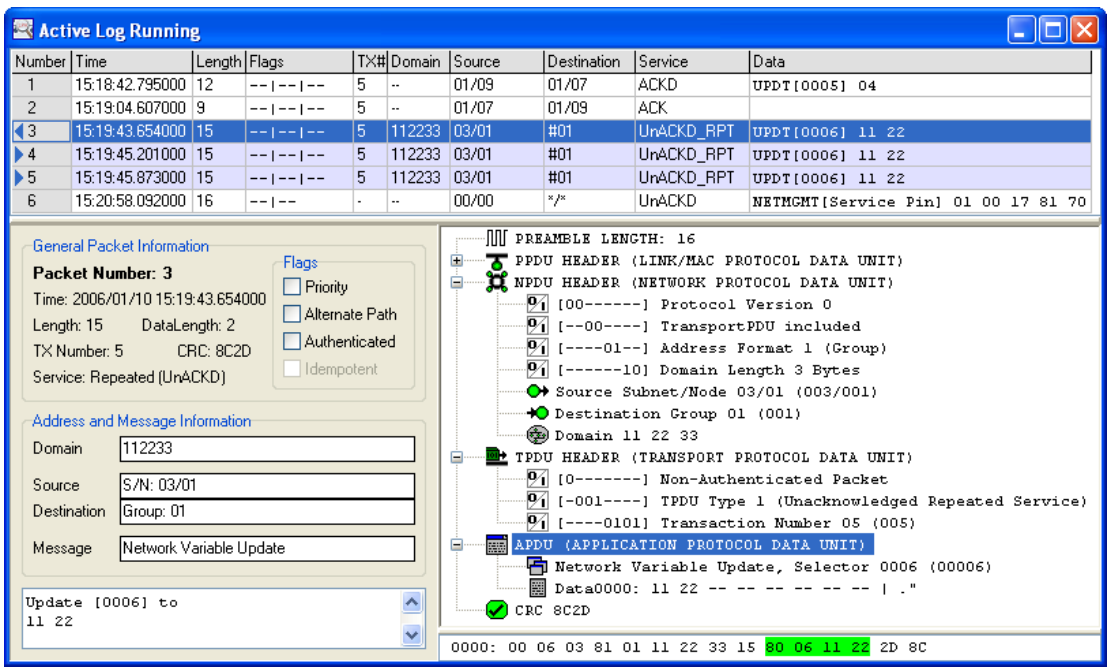
LPA / LPA-IP™

LOYTEC Protocol Analyzer

User Manual

LOYTEC electronics GmbH


Active Log Running
Number Time Length Flags TX# Domain Source Destination Service Data
1 15:18:42.795000 12 --|--|-- 5 -- 01/09 01/07 ACKD UPDT[0005] 04
2 15:19:04.607000 9 --|--|-- 5 -- 01/07 01/09 ACK
3 15:19:43.654000 15 --|--|-- 5 112233 03/01 #01 UnACKD_RPT UPDT[0006] 11 22
4 15:19:45.201000 15 --|--|-- 5 112233 03/01 #01 UnACKD_RPT UPDT[0006] 11 22
5 15:19:45.873000 15 --|--|-- 5 112233 03/01 #01 UnACKD_RPT UPDT[0006] 11 22
6 15:20:58.092000 16 --|-- - -- 00/00 */* UnACKD NETMGMT[Service Pin] 01 00 17 81 70
General Packet Information
Packet Number: 3
Time: 2006/01/10 15:19:43.654000
Length: 15 DataLength: 2
TX Number: 5 CRC: 8C2D
Service: Repeated (UnACKD)
Flags
Priority
Alternate Path
Authenticated
Idempotent
Address and Message Information
Domain 112233
Source S/N: 03/01
Destination Group: 01
Message Network Variable Update
Update [0006] to
11 22
PREAMBLE LENGTH: 16
PPDU HEADER (LINK/MAC PROTOCOL DATA UNIT)
NPDU HEADER (NETWORK PROTOCOL DATA UNIT)
[00------] Protocol Version 0
[--00----] TransportPDU included
[----01--] Address Format 1 (Group)
[------10] Domain Length 3 Bytes
Source Subnet/Node 03/01 (003/001)
Destination Group 01 (001)
Domain 11 22 33
TPDU HEADER (TRANSPORT PROTOCOL DATA UNIT)
[0-------] Non-Authenticated Packet
[-001----] TPDU Type 1 (Unacknowledged Repeated Service)
[----0101] Transaction Number 05 (005)
APDU (APPLICATION PROTOCOL DATA UNIT)
Network Variable Update, Selector 0006 (00006)
Data0000: 11 22 -- -- -- -- -- -- | ."
CRC 8C2D
0000: 00 06 03 81 01 11 22 33 15 80 06 11 22 2D 8C

Contact

LOYTEC
Blumengasse 35
A-1170 Vienna
AUSTRIA/EUROPE
support@loytec.com
http://www.loytec.com

Version 3.3

Document No. 88061214

LOYTEC MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND
LOYTEC SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS PRODUCT IS NOT DESIGNED OR INTENDED FOR USE IN EQUIPMENT INTENDED FOR SURGICAL IMPLANT INTO THE BODY OR OTHER APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH IN THE FAILURE OF SUCH PRODUCT COULD CREATE A SITUATION IN WHICH PERSONAL INJURY OR DEATH MAY OCCUR.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in
any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of LOYTEC.

L-Chip™, LC7093™, L-IP™ and L-Gate™ are trademarks of LOYTEC electronics GmbH.

LonTalk®, LONWORKS®, Neuron®, LONMARK®, LonMaker®, *i*.LON®, and LNS® are trademarks of Echelon Corporation registered in the United States and other countries.

Table of Contents

1 Introduction 5

2 Installation and Setup 6

2.1 Software and Hardware Installation 6

2.2 Network Interface Configuration and Product Registration 6

2.3 Network Interface and Transceiver Selection 6

2.3.1 NIC709-PP, NIC709-USB, and NIC709-PCI Devices 7

2.3.2 NIC852 Devices (LPA-IP) 8

2.3.3 Remote LPA Devices 10

2.3.4 NIC-IP Devices 13

2.3.5 Multiplexed Network Interfaces (MNI Devices) 13

2.4 Command Line File Open 14

2.5 Multiple Configurations 15

2.6 Using several LPAs simultaneously 15

2.7 Server-only mode 15

3 Tutorial 17

4 Using the LPA 21

4.1 LPA Menus 21

4.2 Tool Bar 22

4.3 Log Windows 24

4.4 Status Bar 26

4.5 Find and Go To Packet 27

4.6 Functions of the Popup Menu (View Menu) 27

4.7 Logging Packets from the Network 29

4.8 Packet Log Files 29

4.9 Exporting a Packet Log 30

4.10 Printing a Packet Log 30

4.11 On-line Help System 30

5 Advanced Features of the LPA 31

5.1 Log Mode Settings 31

5.2 Packet Converter 32

5.3 Packet Filters and the Packet Trigger 35

5.4 Display Options 39

5.5 Packet Statistics 41

5.6 Node Statistics 42

5.7 LPA Reports 45

5.8 Statistics Trends 47
5.9 Packet Simulation 48
5.10 Packet Recording Files 49
5.11 LPA Settings 50
6 External Applications 52
6.1 Accessing Data from Packet Recording Files 52
6.2 LPA Server and Clients 52
6.3 LPA Plug-Ins 54
6.4 LPA Report DLLs 55
7 Revision History 57
Abbreviations 58
List of Figures 59
Index 61

1 Introduction

The LOYTEC Protocol Analyzer (LPA) is a powerful tool for analyzing CEA709 and CEA852 / CNIP (Control Network over IP) networks by using a LOYTEC NIC709 or NI852 network interface, which connects your personal computer to the network. After setting up the network interface, incoming packets can be logged and displayed on-line during the logging process. With its filtering, conversion and statistical functions the LPA can extract just the information you want to see. Using the LPA-IP and Remote LPA functionalities, the LPA software can be used to monitor CEA852 networks and remote CEA709 channels from anywhere in the world over the Internet. Further, the LPA can also work in conjunction with external applications (see Chapter 6). For software updates and latest news on the LPA refer to our webpage (http://www.loytec.com).

This manual starts with a description of the LPA installation and setup. A short tutorial is following to help you get started with the LPA software. After that all basic functions as well as advanced features of the protocol analyzer are described. Please observe that the term 'LPA Software' addresses both the LPA-SW and LPA-IP-SW software packages.

2 Installation and Setup

2.1 Software and Hardware Installation

To start the installation process just put the LOYTEC Software CD into your CDR/DVD drive. You might have to run ‘setup.exe’ from the CD if the LOYTEC CD menu does not appear automatically. Please install the latest NIC Software package first by clicking the corresponding menu icon. After installation, please read the NIC User Manual by clicking on the corresponding entry in your Windows Start menu (in ‘LOYTEC Network Interfaces’). It describes in detail how to install and setup your NIC709 or NIC852 network interface hardware.

The next step is to install the LPA Software. Again click on the corresponding menu icon in the LOYTEC CD menu and follow the instructions. For information on Personal Firewall configuration please refer to the NIC User Manual.

2.2 Network Interface Configuration and Product Registration

To configure your LOYTEC network interface, start the LOYTEC configuration tool (‘LConfig’) from your Windows Start menu (in ‘LOYTEC Network Interfaces’). Again refer to the NIC User Manual as well as the LConfig on-line help for more information on network interface configuration.

To register your LPA software please start the LConfig tool, click on 'Register', and type in the Registration Code that comes with your LPA software package. Click on 'Add' and then on 'OK'. If you want to register several LOYTEC products at a time, just enter all registration codes as described. You can also export your set of registration codes to a file and import it in all subsequent installations. Please observe that you must have administrator rights to enter registration codes within the LConfig tool.

2.3 Network Interface and Transceiver Selection

When you start the LPA Software for the first time, in order to start a packet log from your network interface, you must select your network interface as well as the active transceiver. To select a network interface, please click on the button ‘NI’ or select [menu Profile | Network Interface…]. All installed network interface devices will be displayed as shown in Figure 1.

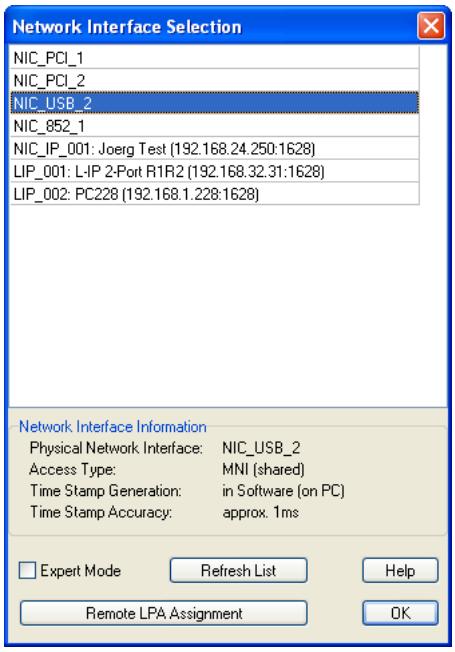


Figure 1: **Network Interface Selection**

If an installed device is missing, please start the LConfig tool and test the network interface. If a specific network interface is not available ('Device not available') it is already in use by a different application. When you click on a network interface, additional information is displayed at the bottom of the dialog window, see also Section 2.3.5. Select your network interface by double clicking on the corresponding line or clicking on 'OK'. You can refresh the list of network interfaces by clicking on 'Refresh List'. Further, you can switch between Standard and Expert Mode for Multiplexed Network Interfaces (see Section 2.3.5) as well as assign Remote LPA Devices (see Section 2.3.3).

After selecting the network interface a transceiver must be selected via [menu Profile | Interface Settings...] or by clicking on the button 'IF'. The corresponding dialog window as well as further specifics of the different network interface types are described in the following sections.

2.3.1 NIC709-PP, NIC709-USB, and NIC709-PCI Devices

This section covers the NIC709 network interface series (except NIC709-IP) as well as all older network interface types labeled 'LPA006', 'LPA-PP', and 'LPA-USB'. These network interfaces connect your PC directly to an CEA709 network. Figure 2 shows the setup for a NIC709-USB as an example.

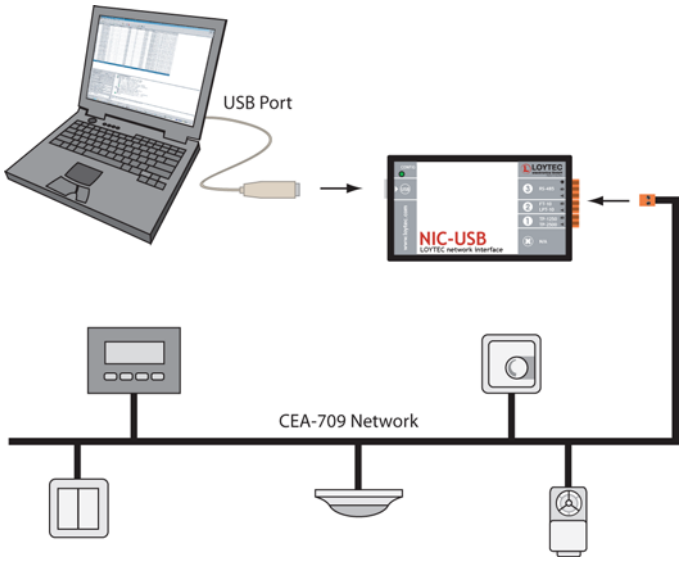


Figure 2: **NIC709 Setup**

The CEA709 network must be connected to the matching transceiver of the NIC709 network interface. This transceiver must then be selected in the 'Interface Settings' dialog within the LPA Software. Figure 3 shows the dialog window for NIC709 network interfaces.

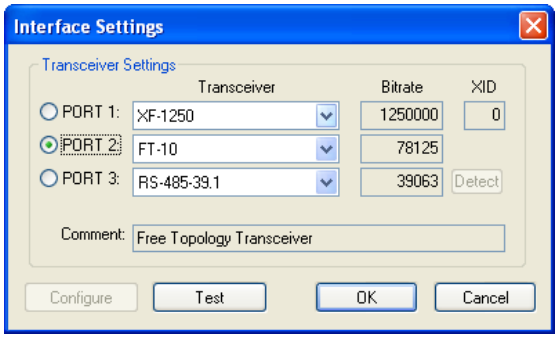


Figure 3: **NIC709 Transceiver Selection**

For each of the three ports a transceiver can be chosen and the corresponding bit-rate will be displayed. You have to select one of the ports as currently active by clicking on the small button on the left side. By clicking on the button 'Test' you can test if the network interface works correctly. For the RS-485 transceivers (Port 3) you can also try automatic bit-rate detection. After clicking on 'Detect' the network is searched for traffic using different bit-rates. The correct bit-rate can only be detected if packets are received during the detection process.

2.3.2 NIC852 Devices (LPA-IP)

When purchasing an LPA-IP package, you will receive a small NIC852 USB key for enabling the PC to connect to an CEA852 / CNIP (Control Network over IP) network. The standard use case for the NIC852 is to function as a member (node) on an CEA852 / CNIP channel (LonMark IP-852), see Figure 4.

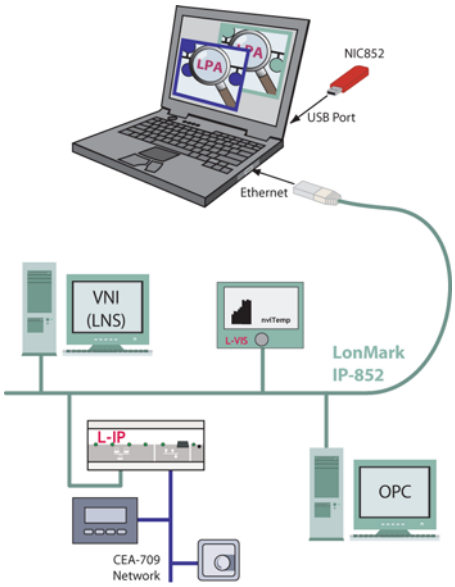


Figure 4: **LPA-IP running on NIC852**

In this case the LPA-IP-SW software receives the complete traffic of the IP-852 channel. Refer to the NIC User Manual on how to configure the NIC852 to become a member of an CEA852 channel. Please keep in mind that due to the point-to-point nature of CEA852, the packet log as seen in the LPA might not exactly represent the communication between nodes in some situations. Figure 5 illustrates why this is the case.

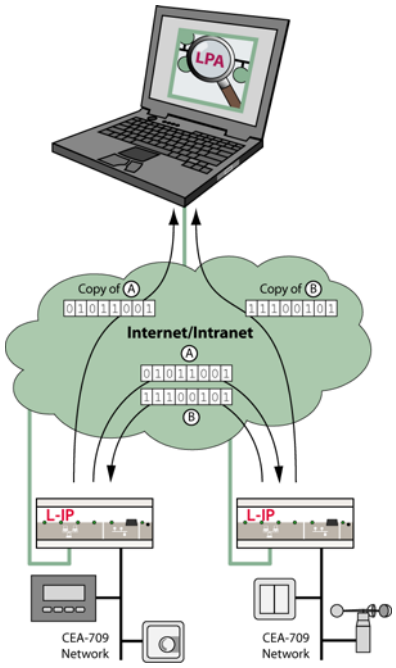


Figure 5: **CEA852 Packet Logging**

When an LPA is inserted into an existing CEA852 channel, all members are automatically informed of the new member and start to send *copies* of all packets to the LPA. In Figure 5 e.g., the left L-IP sends packet A to the right L-IP and a *copy* of packet A to the LPA. The right L-IP sends packet B to the left L-IP and a *copy* of packet B to the LPA. Thus, it is possible that the packet order of some transactions is mixed up in the LPA packet log window (e.g. showing a Response <B> before the Request <A>). It might also be possible, that the copy of a packet is seen in the LPA, but the original packet

- has not reached its destination,
- was discarded at the destination due to a not properly set channel timeout value, or
- a not synchronized system clock,

and vice versa. This could mainly be the case in WANs (Wide Area Networks), where packet transmission time from different nodes can vary significantly and packets can even be lost. Additionally, the accuracy of the packet time stamps shown in the LPA is also largely dependent on IP packet propagation delay. However, in a LAN (Local Area Network), these effects should be minimal.

Figure 6 shows the 'Interface Settings' dialog window of the LPA software for NIC852. Here you can choose between IP-10L (LAN) and IP-10W (WAN).

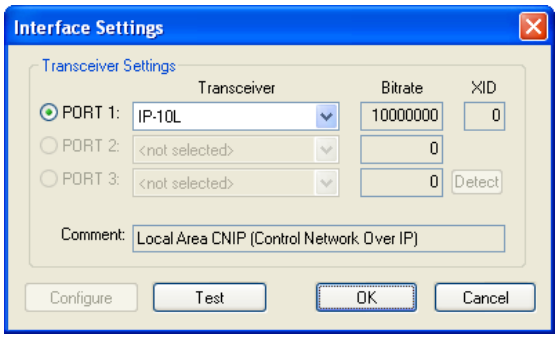


Figure 6: **NIC852 Transceiver Selection**

Another use case for the NIC852 is to connect directly to a Remote LPA device and log packets from the CEA709 port of the device, as described in Section 2.3.3.

2.3.3 Remote LPA Devices

The LPA-IP-SW software in combination with a NIC852 can be used to log packets from the CEA709 port of a specific device with Remote LPA functionality (e.g. LOYTEC L-IP Router). In this use case, the PC is not necessarily a member of the corresponding CEA852 channel (although it could be). Rather, the LPA-IP is connected to the remote device over the Internet/Intranet in a point-to-point fashion.

In the example of Figure 7, two LPA logs are started, one on each L-IP device. Each LPA log window shows the local traffic of the corresponding L-IP's CEA709 port. To discover and assign Remote LPA devices for the LPA-IP-SW software, a 'Remote Device Discovery and Assignment' module is available, which can be invoked by clicking on 'Remote LPA Assignment' in the Network Interface selection dialog (see Figure 1). Figure 8 shows the Remote LPA Assignment dialog window.

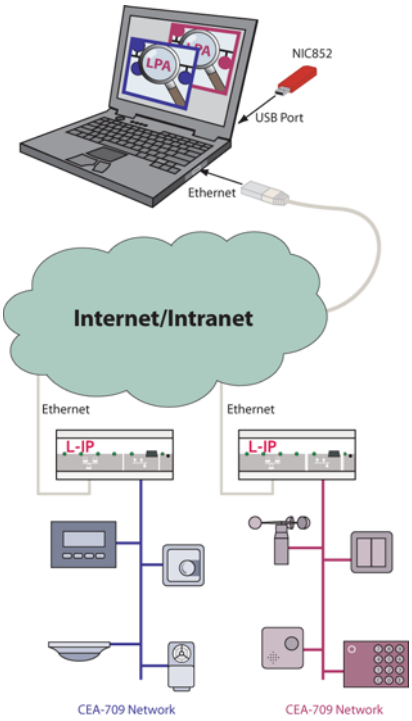


Figure 7: **Remote LPA running on L-IP**

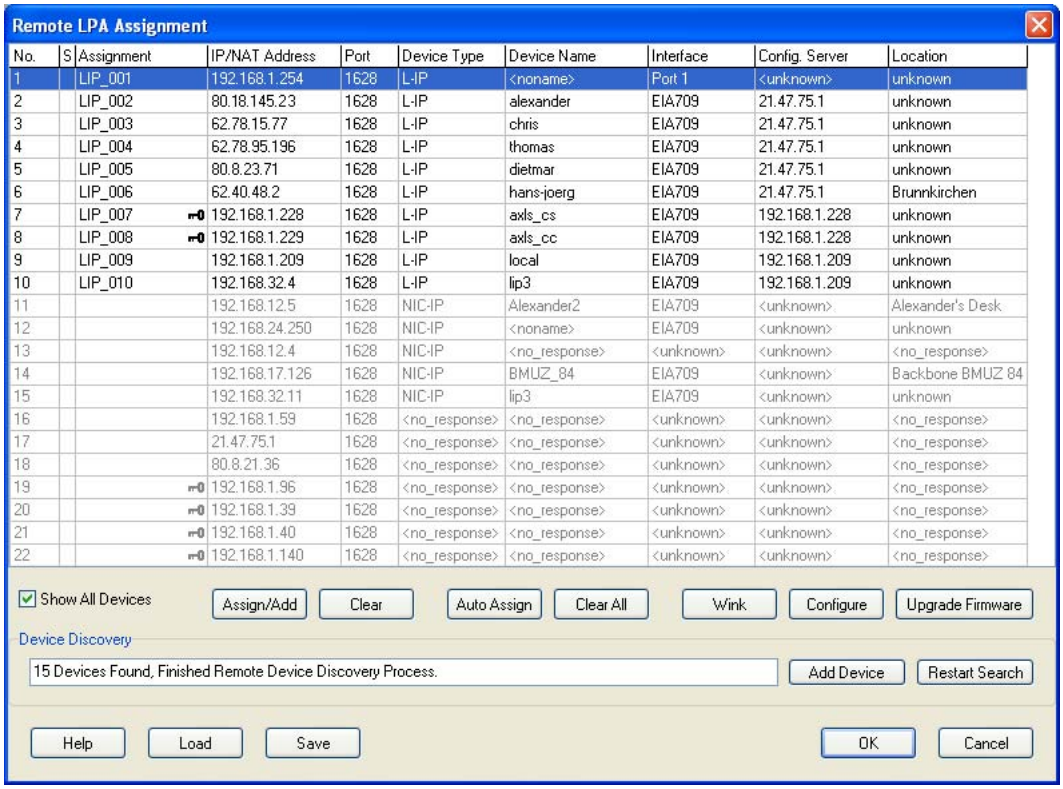


Figure 8: **Remote LPA Assignment**

In the device table all discovered devices will be displayed. All devices without Remote LPA function as well as devices that cannot be contacted will be displayed gray. Use the checkbox ‘Show All Devices’ to decide whether to see all remote devices or just the Remote-LPA devices. During device discovery, already discovered devices can be assigned immediately. It is not necessary to wait for the completion of the discovery process since this can be a lengthy procedure depending on the size of the scanned channel(s).

To assign a Remote LPA device please select the corresponding line of the device table and click on ‘Assign/Add’ or just double-click on the device to assign. To add a device not present in the device table, also click on ‘Assign/Add’. The dialog box shown in Figure 9 will appear.

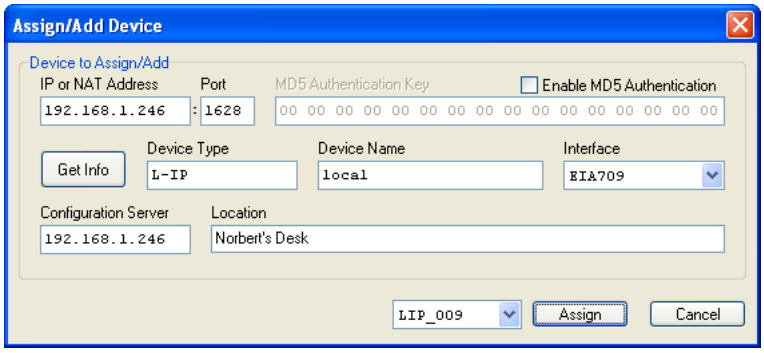


Figure 9: **Assign/Add Remote LPA Device**

You can change the IP address and port manually in the fields ‘IP or NAT Address’ and ‘Port’. When the device is located behind a NAT router, you must enter the IP address of the NAT router. If MD5 is enabled in the device, you must check ‘Enable MD5 Authentication’ and enter the correct ‘MD5 Authentication Key’. MD5 authentication is indicated by a small key symbol in the ‘Assignment’ column of the device list, as shown in Figure 8. Before assigning the device you can click on ‘Get Info’ to check the device name, type, interface list, configuration server and location string. Finally select a logical device (LIP_001 … LIP_512) and click on ‘Assign’ to assign the device.

To automatically assign all currently discovered devices, click on ‘Auto Assign’ in the Remote LPA Assignment dialog (Figure 8). You can sort the discovered devices first by clicking on a specific column header in the device table. The assignments can be cleared, loaded and saved using the buttons ‘Clear’, ‘Clear All’ ‘Load’, and ‘Save’. If no remote devices are discovered or you want to add another CEA852 channel, please click on ‘Add Device’, which opens the dialog window depicted in Figure 10.

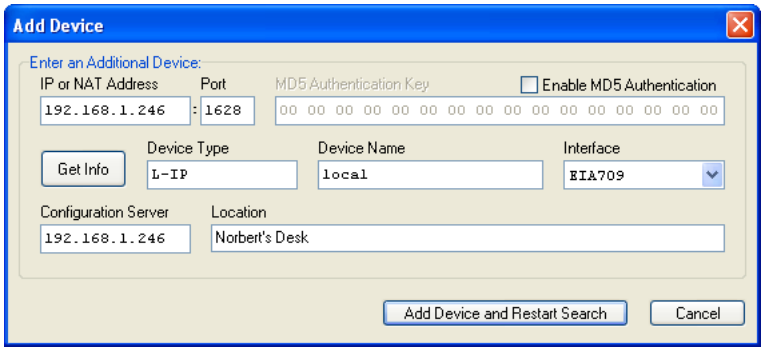


Figure 10**: Add CEA852 Channel**

Just like in the ‘Assign/Add’ dialog, please enter the IP/NAT address, the port number and (optionally) the MD5 key of one channel member. You can click on ‘Get Info’ to see if the chosen device can be contacted. Finally, click on ‘Add Device and Restart Search’. All members of the added channel should now be displayed in the Remote LPA Assignment dialog. Note that you must assign at least one member of the new channel to add the channel persistently.

By clicking on ‘Wink’ you can make the selected device blink with some LEDs in different colors. This can be used to locate a specific device in the network. When all devices are assigned, click on ‘OK’. In the Network Interface selection dialog the assigned devices will appear as ‘LIP_001’, ‘LIP_002’, etc., see Figure 1.

It is not necessary to select a transceiver for Remote-LPA devices since the transceiver is determined by the physical configuration of the device. However, when the 'Interface Settings' dialog is invoked, it shows the CEA709 transceiver for the currently selected device, see Figure 11. The 'PORT' in this case is only a property of the physical transceiver connection on the device and can therefore be ignored.

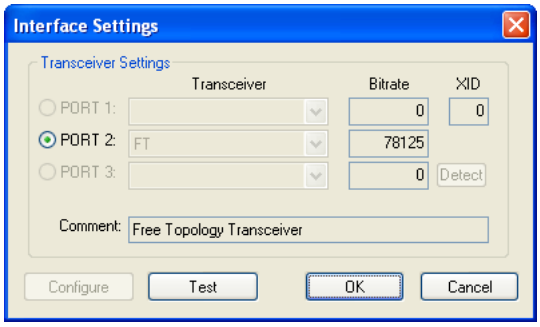


Figure 11: **Transceiver Display for Remote-LPA Devices**

Note that the time stamps shown in the packet log window for a Remote LPA device are generated within the device (local time of the device). If the time stamps are incorrect, please make sure to adjust the time in the observed device. Refer to the corresponding device documentation for more information.

2.3.4 NIC-IP Devices

All NIC-IP related settings are now done in the L-Config tool, see NIC User Manual.

2.3.5 Multiplexed Network Interfaces (MNI Devices)

The NIC-PCI, NIC-USB, NIC-IP, and NIC852 network interfaces can be used in a 'Multiplexed Network Interface' mode. Each physical network interface is represented by 8 Multiplexed Network Interfaces (MNI devices). This means that you can start up to 8 different applications running on the same physical network interface at a time. These 'virtual interfaces' behave like nodes on a 'virtual channel' connected to the physical channel via the physical network interface, as depicted in Figure 12.

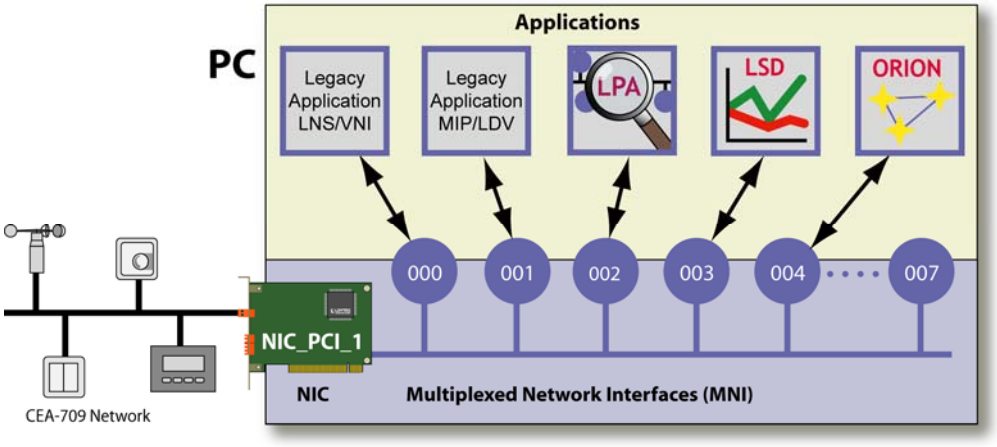


Figure 12: **Multiplexed Network Interfaces**

You could e.g. run the LPA software, the LSD tool, a custom ORION application, an LNS/VNI application, and a MIP/LDV application at the same time using only one NIC709-PCI network interface.

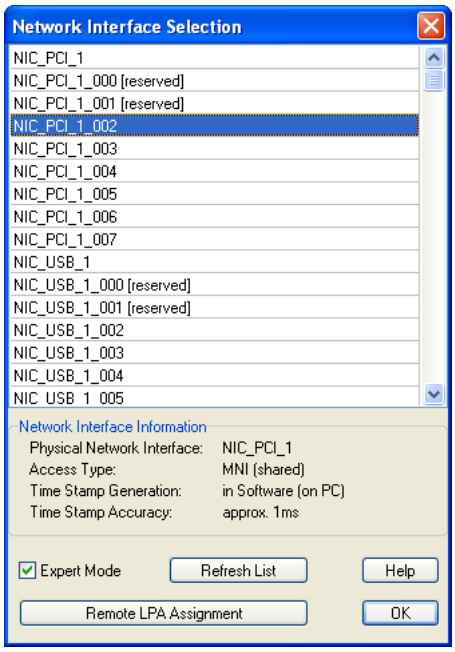


Figure 13: **Expert Mode for Network Interface Selection**

When using the Standard Mode ('Expert Mode' disabled, see Figure 1) in the Network Interface selection dialog, MNI devices are automatically used if supported by the network interface. This way, both the LPA and the LSD software can e.g. run on the same network interface 'NIC_PCI_1'. In 'Expert Mode', the physical network interface (e.g. 'NIC_PCI_1') as well as all corresponding MNI devices ('NIC_PCI_1_000', 'NIC_PCI_1_001', 'NIC_PCI_1_002', etc.) are displayed and can be selected explicitly, see Figure 13. The [reserved] devices are reserved for Legacy applications and should not be selected, see NIC User Manual. Following is a list of differences between physical devices and MNI devices:

- All MNI devices share the same serial number (equal to the serial number of the physical network interface).

- If the physical device is already occupied, the MNI devices for that physical device are not available and vice versa.

- LPA time stamps are calculated in software when logging from an MNI device (rather than generated in hardware when logging from the physical device) and therefore have a lower resolution.

The physical network interface name, the access type, as well as information about timestamp generation is displayed at the bottom of the network interface selection window, as shown in Figure 1 and Figure 13. Other than that, the behavior of an MNI device is exactly the same as of a physical network interface. It is completely transparent to the LPA software if the underlying network interface is multiplexed or not. Please note that the NIC Legacy Driver must be running to enable MNI devices.

2.4 Command Line File Open

To open a packet log file when starting the LPA, the command line parameter '-f' can be used:

e.g.: 'C:\Program Files\LOYTEC\LPA\LPA.exe -f log_name1.plg'

Note that after installation of the LPA software, packet log files (*.plg) can also be opened by double-clicking them in the explorer.

2.5 Multiple Configurations

By using a command line parameter, different independent LPA configurations can be setup. If you want to create a new LPA configuration just create a shortcut to the executable file ('LPA.exe') e.g. on your desktop and choose properties (by clicking the right mouse button on the LPA icon). Then go to 'Shortcut' and append a unique configuration name in the 'Target'-field:

e.g.: 'C:\Program Files\LOYTEC\LPA\LPA.exe' ⇒

'C:\Program Files\LOYTEC\LPA\LPA.exe ConfigName1'

The name of the LPA icon should also be changed accordingly to be able to distinguish the LPA icons from each other. You can repeat this procedure with different configuration names to create several independent LPA configurations. All settings done within the LPA software will then only affect the configuration of the LPA icon you have used to start the software. All other configurations remain unchanged.

2.6 Using several LPAs simultaneously

If you want to observe more than one network channel at a time, you can use several instances of the LPA software simultaneously. Just start the LPA software for each device you want to log packets from. Observe that you have to choose the correct network interface (see Section 2.3) for each LPA software you start. To avoid changing these settings upon every program start, just create several different LPA configurations (one for each network interface) as described in Section 2.4.

2.7 Server-only mode

The LPA Software can be started in a Server-only mode. Please refer to Section 6.2 for more information on the LPA Server function. In the Server-only mode, the LPA automatically starts a packet log and forwards all packets (passing the capture filter) to LPA Clients. To activate the Server-only mode, the LPA must be started with the option '-s'. To distinguish the LPA Server-only configuration from the normal LPA configuration (or other custom configurations, see Section 2.4), it is recommended to assign a certain configuration name to the Server-only configuration. The LPA would then be started e.g. like this:

'C:\Program Files\LOYTEC\LPA\LPA.exe ServerConfig -s'

A corresponding shortcut could be put in the Autostart folder of the Windows start menu to automatically start the LPA Server at boot time. Since there is no graphical user interface available in Server-only mode, you must setup the LPA (network interface, packet converter, capture filter, etc.) beforehand by starting the LPA without the '-s' option but still with the Server-only configuration name:

'C:\Program Files\LOYTEC\LPA\LPA.exe ServerConfig'

The configuration is saved automatically when exiting the LPA. When the LPA is started in Server-only mode, a systray icon will appear, which shows the state of the LPA Server, see Figure 14.

Figure 14: **LPA Server Systray Icon**

The color of the icon indicates the following states:

- Gray … Inactive (Paused) or trying to open Network Interface
- Green … Active (Running)
- Red … An error has occurred

When the mouse is moved over the icon, additional information about the current state of the LPA Server is displayed. Further, a popup menu is available, which appears when right-clicking the systray icon, see Figure 15.

Figure 15: **Systray Icon Menu**

By double-clicking the systray icon or choosing ‘Pause’ in the menu, you can pause and restart the LPA Server. When an error has occurred upon startup, you can retry to startup the LPA Server by choosing ‘Start’. With ‘Exit’, you can terminate the LPA Server.

3 Tutorial

This tutorial is meant to help you get familiar with the main features of the LPA. A detailed description of all functions is provided in the chapters 4 and 5. The steps that are explained here can be performed without the need of an actual network.

1.) *Start the LPA and click on the button* .

You have created a new log window to display incoming packets. It is called 'Active Log' as shown in Figure 16.

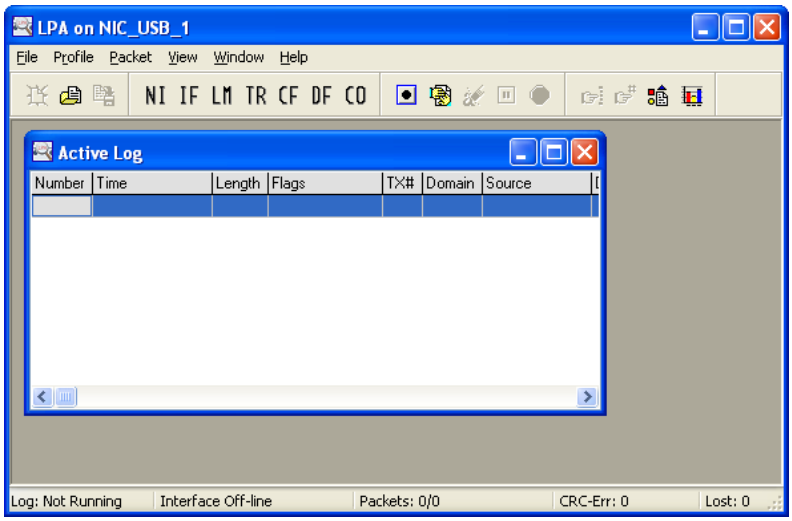


Figure 16: **Active Log Window**

2.) *Start the logging process by selecting* [menu Packet | Start Log | from File (trace)...].

Packets will be logged from a file to simulate a real network. An open-dialog box is shown where you open the file 'tutorial.prc' that comes with the LPA. Watch the log window where packets appear now. Every incoming packet occupies a line of the table as shown in Figure 17.

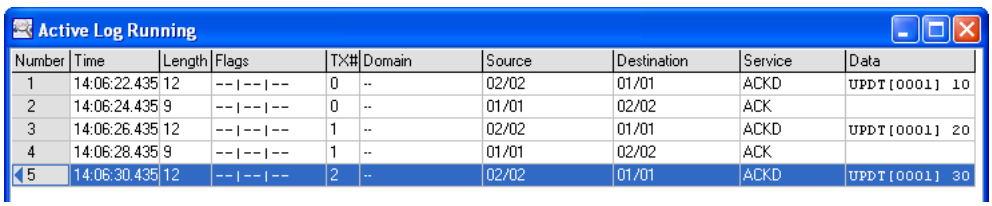


Figure 17: **Incoming Packets**

3.) *Pause the logging process by clicking on* .

4.) *Click on the right mouse button within the log window and choose* 'Packet Details'.

Whenever you click on the right mouse button within a log window, a popup menu will appear where you can setup the packet display. Detailed information about the currently active packet is displayed now as shown in Figure 18.

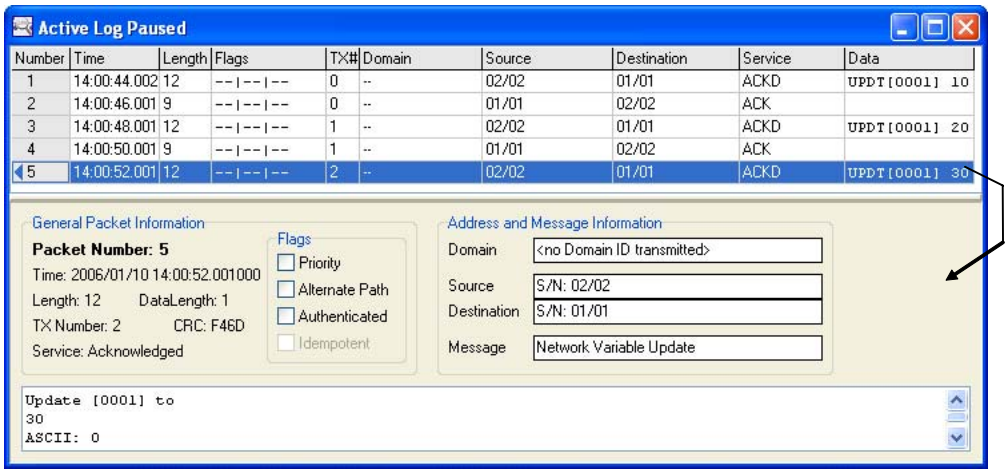

Active Log Paused
Number Time Length Flags TX# Domain Source Destination Service Data
1 14:00:44.002 12 --|--|-- 0 -- 02/02 01/01 ACKD UPDT[0001] 10
2 14:00:46.001 9 --|--|-- 0 -- 01/01 02/02 ACK
3 14:00:48.001 12 --|--|-- 1 -- 02/02 01/01 ACKD UPDT[0001] 20
4 14:00:50.001 9 --|--|-- 1 -- 01/01 02/02 ACK
5 14:00:52.001 12 --|--|-- 2 -- 02/02 01/01 ACKD UPDT[0001] 30
General Packet Information
Packet Number: 5
Time: 2006/01/10 14:00:52.001000
Length: 12 DataLength: 1
TX Number: 2 CRC: F46D
Service: Acknowledged
Flags
Priority
Alternate Path
Authenticated
Idempotent
Address and Message Information
Domain <no Domain ID transmitted>
Source S/N: 02/02
Destination S/N: 01/01
Message Network Variable Update
Update [0001] to
30
ASCII: 0

Figure 18: **Packet Details**

5.) *Click on the right mouse button within the log window and choose* 'Protocol Details'.

Details of all information contained in the current packet according to the network protocol is displayed now (see Section 4.3). You can switch off packet details and protocol details again by repeating steps 4 and 5.

6.) *Edit the packet converter by clicking on* .

A dialog box appears where you click on the button 'Open' and choose the file 'tutorial.pco'. The packet converter is used to display symbolic names instead of plain numbers (for addresses and network variables) in the log window. Click on the button 'OK' now. The columns 'Domain', 'Source', 'Destination' and 'Data' in the log window are changed according to the conversion tables as shown in Figure 19.

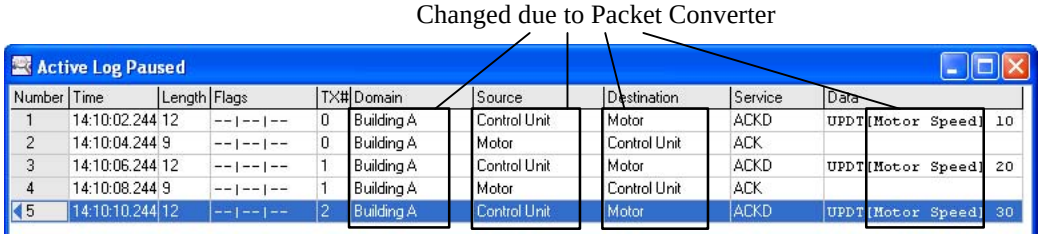

Changed due to Packet Converter
Active Log Paused
Number Time Length Flags TX# Domain Source Destination Service Data
1 14:10:02.244 12 --|--|-- 0 Building A Control Unit Motor ACKD UPDT[Motor Speed] 10
2 14:10:04.244 9 --|--|-- 0 Building A Motor Control Unit ACK
3 14:10:06.244 12 --|--|-- 1 Building A Control Unit Motor ACKD UPDT[Motor Speed] 20
4 14:10:08.244 9 --|--|-- 1 Building A Motor Control Unit ACK
5 14:10:10.244 12 --|--|-- 2 Building A Control Unit Motor ACKD UPDT[Motor Speed] 30

Figure 19: **Converted Packets**

7.) *Edit the packet display filter by clicking on* .

The packet display filter decides which of the logged packets shall be displayed. By default all packets can pass the filter and are shown in the log window. To get an idea how a packet filter works enable the filter by clicking on 'Enable Display Filter'. Next click on the 'Layer 4' filter section and enable the checkbox 'Enable TPDU Filter'. Now you can

setup filter parameters on layer 4 of the network protocol. Disable the checkbox ‘Acknowledgements’ to hide all acknowledgment packets in the log window. When you click on ‘OK’, the changes you have performed in the display filter will take effect and acknowledgments will be hidden.

8.) *Deactivate the display filter by clicking on* *and disabling ‘Enable Display Filter’.*

After clicking on ‘OK’, all packets will be shown again. The whole display filter is now disabled and all captured packets are displayed in the log window.

Note that there is also a packet capture filter available. It decides whether incoming packets shall be stored in memory or be discarded. This is done prior to display filtering (see Section 5.3).

9.) *Restart the logging process by clicking on* .

10.) *Show the packet statistics by clicking on* .

The window shown in Figure 20 will appear. It displays various packet statistics information (see Section 5.5).

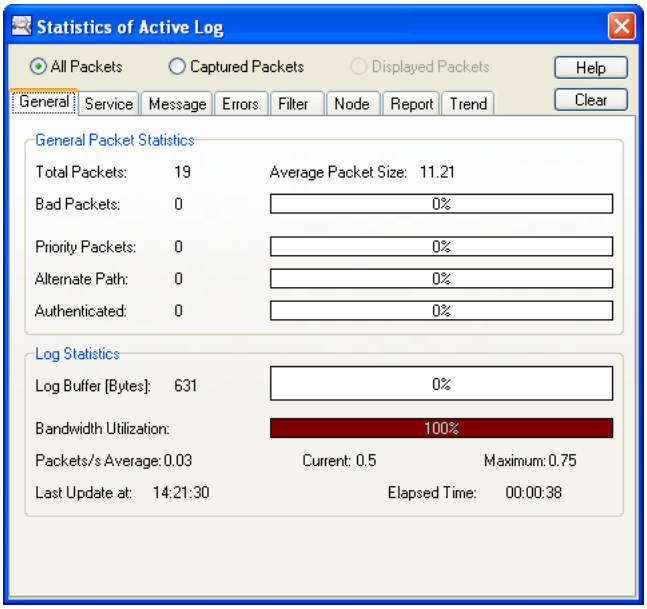


Figure 20: **Packet Statistics Window**

11.) *Wait till all packets are logged from the demonstration file* ‘tutorial.prc’.

When all packets are logged, the dialog box shown in Figure 21 will appear where you click on ‘OK’. You can also stop the logging process manually by clicking on .

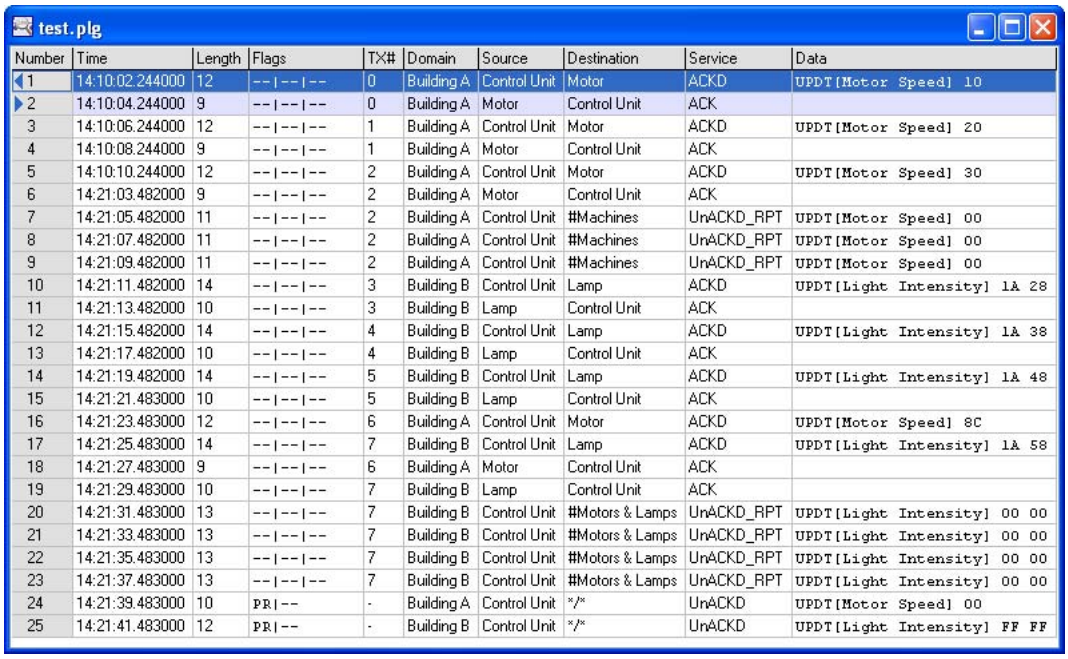
Figure 21: **End of Demonstration Log**

12.) *Store the packet log by clicking on* .

A save-dialog box is invoked where you save the log under the name ‘test.plg’. After that you can close the packet log by selecting [menu File | Close]. You will be prompted to ‘Save Changes to Display Filter’ where you click on ‘No’.

13.) *Open the just stored packet log by clicking on* .

An open-dialog box appears where you open the file ‘test.plg’. Observe that the used packet converter file (‘tutorial.pco’) is also opened automatically. Figure 22 shows the packet log window which should appear on your screen. You can now further analyze the packet log or exit the LPA by selecting [menu File | Exit].



test.plg

Number	Time	Length	Flags	TX#	Domain	Source	Destination	Service	Data
1	14:10:02.244000	12	--|--|--	0	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 10
2	14:10:04.244000	9	--|--|--	0	Building A	Motor	Control Unit	ACK	
3	14:10:06.244000	12	--|--|--	1	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 20
4	14:10:08.244000	9	--|--|--	1	Building A	Motor	Control Unit	ACK	
5	14:10:10.244000	12	--|--|--	2	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 30
6	14:21:03.482000	9	--|--|--	2	Building A	Motor	Control Unit	ACK	
7	14:21:05.482000	11	--|--|--	2	Building A	Control Unit	#Machines	UnACKD_RPT	UPDT[Motor Speed] 00
8	14:21:07.482000	11	--|--|--	2	Building A	Control Unit	#Machines	UnACKD_RPT	UPDT[Motor Speed] 00
9	14:21:09.482000	11	--|--|--	2	Building A	Control Unit	#Machines	UnACKD_RPT	UPDT[Motor Speed] 00
10	14:21:11.482000	14	--|--|--	3	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 28
11	14:21:13.482000	10	--|--|--	3	Building B	Lamp	Control Unit	ACK	
12	14:21:15.482000	14	--|--|--	4	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 38
13	14:21:17.482000	10	--|--|--	4	Building B	Lamp	Control Unit	ACK	
14	14:21:19.482000	14	--|--|--	5	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 48
15	14:21:21.483000	10	--|--|--	5	Building B	Lamp	Control Unit	ACK	
16	14:21:23.483000	12	--|--|--	6	Building A	Control Unit	Motor	ACKD	UPDT[Motor Speed] 8C
17	14:21:25.483000	14	--|--|--	7	Building B	Control Unit	Lamp	ACKD	UPDT[Light Intensity] 1A 58
18	14:21:27.483000	9	--|--|--	6	Building A	Motor	Control Unit	ACK	
19	14:21:29.483000	10	--|--|--	7	Building B	Lamp	Control Unit	ACK	
20	14:21:31.483000	13	--|--|--	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
21	14:21:33.483000	13	--|--|--	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
22	14:21:35.483000	13	--|--|--	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
23	14:21:37.483000	13	--|--|--	7	Building B	Control Unit	#Motors & Lamps	UnACKD_RPT	UPDT[Light Intensity] 00 00
24	14:21:39.483000	10	PR|--	-	Building A	Control Unit	*/*	UnACKD	UPDT[Motor Speed] 00
25	14:21:41.483000	12	PR|--	-	Building B	Control Unit	*/*	UnACKD	UPDT[Light Intensity] FF FF

Figure 22: **Log Window of Packet Log File**

4 Using the LPA

The LOYTEC Protocol Analyzer enables you to monitor and analyze packets from a network by capturing packets from the net and storing them into packet logs. The LPA is an application with a *Multi Document Interface* (MDI) which means that several documents (packet logs) can be open at a time. These packet logs can be stored to packet log files. There is one special packet log called the 'Active Log'. This is the log window where packets are logged in. There can only be one active log at a time. An active log window is created by selecting [menu File | New] or by clicking on the button . Figure 23 shows the main window of the LPA with two open log files.

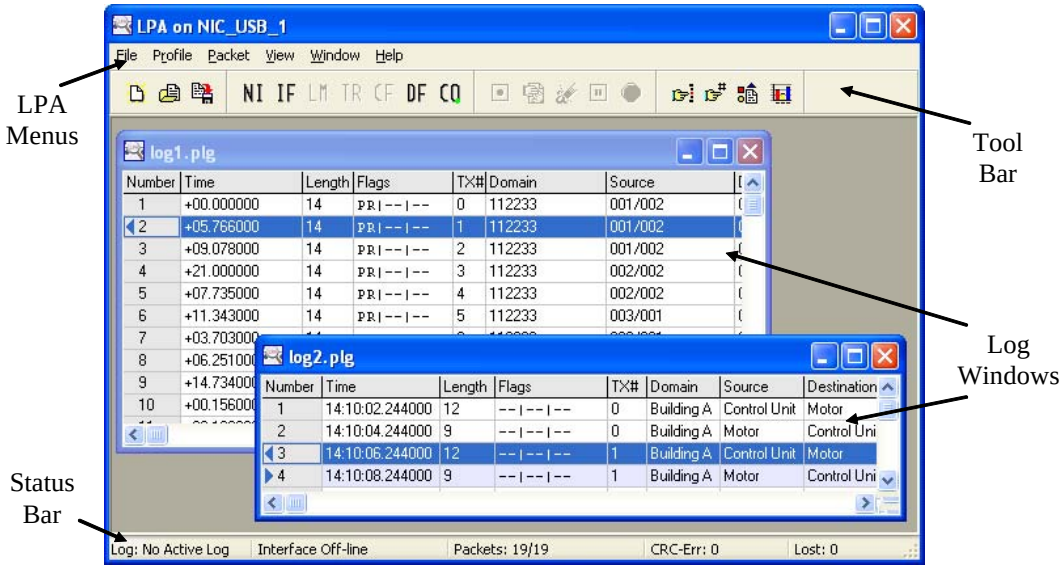


Figure 23: **Main Window of the LPA**

4.1 LPA Menus

Here you can select the functions of the LPA. Shortcut keys are available for most of the menu items. They appear next to the corresponding item when a menu is activated. There are five main menus which contain the following groups of functions:

File Menu: log file processing and general settings,

Profile Menu: interface and log setup,

Packet Menu: packet logging and analysis,

View Menu: same as popup menu, see Section 4.6,

Window Menu: arrangement of log windows and selection of visible log window,

Help Menu: on-line help system and information about LPA.

Some menu items are disabled (dimmed) when it is not allowed to activate the corresponding function for some reason. When a specific function of the LPA is described in the following, the menu item to activate this function is always mentioned.

4.2 Tool Bar

Some common functions of the LPA can be activated by clicking on the buttons of the tool bar to provide quick access. When the mouse pointer is positioned over one of the buttons a small box showing the corresponding menu item appears as illustrated in Figure 24.

Figure 24: **Button and Corresponding Menu Item**

Some buttons are disabled whenever the linked menu items are disabled. The tool bar consists of the following buttons:

New Log [menu File | New]: Creates a new window for the active log. This is used whenever new packets shall be logged from the network or from other sources the analyzer can utilize (see Chapter 5).

Open Log [menu File | Open...]: Opens a previously stored log file.

Save Log [menu File | Save]: Stores the current log to a log file. To store the current log under a new name select [menu File | Save As...].

Network Interface [menu Profile | Interface...]: Allows you to select the network interface (see Chapter 2)

Interface Settings [menu Profile | Interface...]: Allows you to setup the network interface (see Chapter 2)

Log Mode [menu Profile | Log Mode...]: Allows you to setup the log mode for the active log prior to starting the packet capturing process (see Section 5.1).

Trigger [menu Profile | Trigger...]: Allows you to setup a packet trigger for the active log. It decides when to start the packet capturing process (see Section 5.3). A small green point on the button indicates that the packet trigger is enabled.

Capture Filter [menu Profile | Capture Filter...]: Allows you to setup a packet capture filter for the active log. During the logging process the capture filter decides whether to store an incoming packet or discard it (see Section 5.3). A small green point on the button indicates that the capture filter is enabled.

Display Filter [menu Profile | Display Filter...]: Allows you to setup a packet display filter for the current log. The display filter decides which of the captured packets are actually displayed in the log window (see Section 5.3). A small green point on the button indicates that the display filter is enabled.

Converter [menu Profile | Converter...]: Allows you to setup a packet converter for the current log. The packet converter is used to display symbolic names instead of plain numbers contained in the packets (see Section 5.2). A small green point on the button indicates that a packet converter is active.

Start Log from Network [menu Packet | Start Log | Network]: Starts the packet capturing process for the active log. Packets are logged from the connected network until the log is paused or stopped. Note that a log can only be started if an active log window is present.

Pause Update [menu Packet | Pause Update]: Disables display updates of the active log window, the packet statistics (see Section 5.5) and the status bar during the logging process.

Clear Log [menu Packet | Clear Log]: Deletes all packets from the active log. This is only possible when the log is paused (see next button).

Pause Log [menu Packet | Pause Log]: Pauses the packet capturing process until the button is clicked again. While the active log is paused, converter and filter parameters as well as display options can be changed (see Chapter 5).

Stop Log [menu Packet | Stop Log]: Stops the packet capturing process. The active log gets inactive and can then be stored to a packet log file. To start the logging process again, a new log window has to be created.

Find [menu Packet | Find...]: Allows you to search for a specific packet in the current log window. To continue searching after a matching packet has been found, you have to press F3 or select [menu Packet | Find Next].

Go To [menu Packet | Go To...]: Allows you to jump to a specific packet by entering the line number of the packet within the packet table (see following section).

Display Options [menu View | Display Options...]: Allows you to setup display options which affect the appearance of information in the current log window (see Section 5.4).

Statistics [menu Packet | Statistics]: Shows packet statistics for the current log. Includes node statistics, reports, and trends.

Note that the packet trigger, capture filter and display filter can be enabled and disabled by clicking the right mouse button on the corresponding tool bar button or by editing the corresponding filter form (left mouse button).

4.3 Log Windows

These are the windows that display packet data in various forms. They consist of up to three areas as shown in Figure 25.

Packet Table

This is the scrolling list of packets displayed in the top area of the log window. It is always visible and shows the most essential information about each packet where every row of the table represents a packet. The information that can be viewed includes:

- *Number*: line number of packet,
- *Time*: time stamp (when packet was logged),
- *Length*: packet length in bytes,
- *Flags*: packet flags (Priority | Alternate Path | Authenticated | Idempotent),
- *TX#*: transaction number if included in the frame,
- *Domain*: domain in which packet was sent,
- *Source*: source address of packet,
- *Destination*: destination address of packet,
- *Service*: service being used to transport the packet message (data),
- *Data*: message (data) transported in the packet.

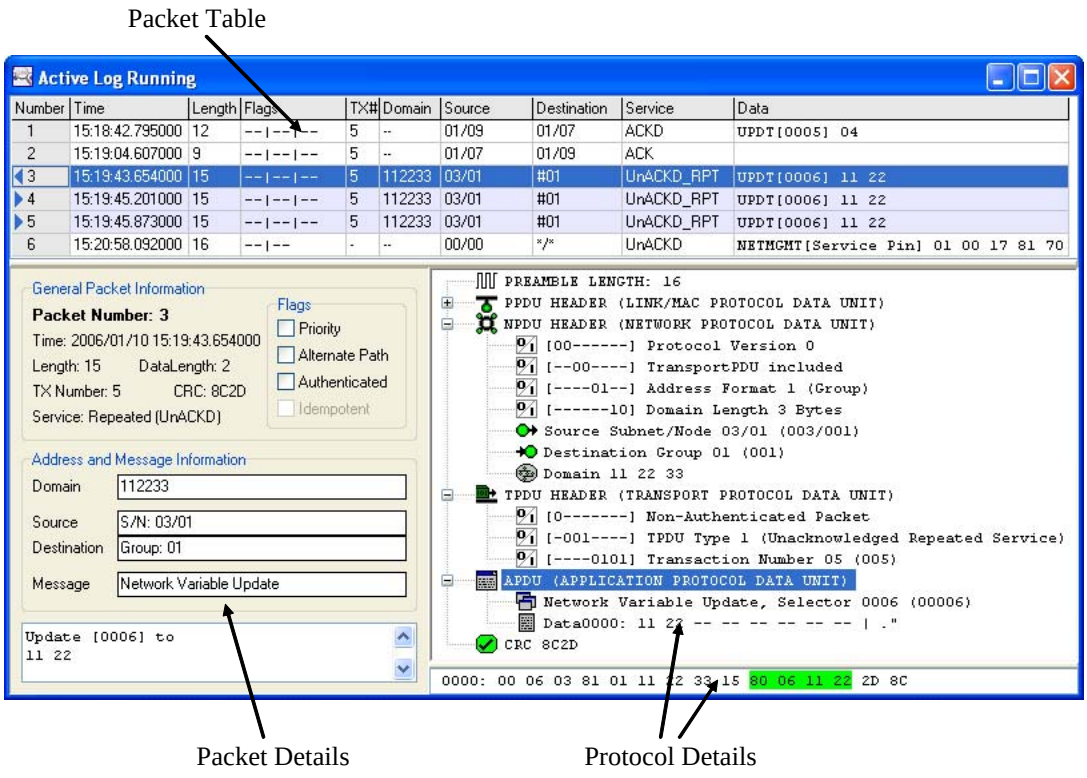

Packet Table
Active Log Running
Number Time Length Flags TX# Domain Source Destination Service Data
1 15:18:42.795000 12 --|--|-- 5 -- 01/09 01/07 ACKD UPDT[0005] 04
2 15:19:04.607000 9 --|--|-- 5 -- 01/07 01/09 ACK
3 15:19:43.654000 15 --|--|-- 5 112233 03/01 #01 UnACKD_RPT UPDT[0006] 11 22
4 15:19:45.201000 15 --|--|-- 5 112233 03/01 #01 UnACKD_RPT UPDT[0006] 11 22
5 15:19:45.873000 15 --|--|-- 5 112233 03/01 #01 UnACKD_RPT UPDT[0006] 11 22
6 15:20:58.092000 16 --|-- - -- 00/00 */* UnACKD NETMGMT[Service Pin] 01 00 17 81 70
General Packet Information
Packet Number: 3
Time: 2006/01/10 15:19:43.654000
Length: 15 DataLength: 2
TX Number: 5 CRC: 8C2D
Service: Repeated (UnACKD)
Flags
Priority
Alternate Path
Authenticated
Idempotent
Address and Message Information
Domain 112233
Source S/N: 03/01
Destination Group: 01
Message Network Variable Update
Update [0006] to
11 22
PREAMBLE LENGTH: 16
PPDU HEADER (LINK/MAC PROTOCOL DATA UNIT)
NPDU HEADER (NETWORK PROTOCOL DATA UNIT)
[00------] Protocol Version 0
[--00----] TransportPDU included
[----01--] Address Format 1 (Group)
[------10] Domain Length 3 Bytes
Source Subnet/Node 03/01 (003/001)
Destination Group 01 (001)
Domain 11 22 33
TPDU HEADER (TRANSPORT PROTOCOL DATA UNIT)
[0-------] Non-Authenticated Packet
[-001----] TPDU Type 1 (Unacknowledged Repeated Service)
[----0101] Transaction Number 05 (005)
APDU (APPLICATION PROTOCOL DATA UNIT)
Network Variable Update, Selector 0006 (00006)
Data0000: 11 22 -- -- -- -- -- -- | ."
CRC 8C2D
0000: 00 06 03 81 01 11 22 33 15 80 06 11 22 2D 8C
Packet Details
Protocol Details

Figure 25: **Log Window**

In the ‘Number’-column, small triangles identify corresponding packets of a transaction. When the triangle is pointed left, it indicates the first packet of the transaction. For subsequent packets, the triangle is pointed right. Further, all packets belonging to the same transaction as the currently selected packet, are marked blue.

Time stamps have a resolution of 1µs for NIC709 network interfaces. Other network interface types may have lower time stamp accuracy, see Section 2.3. Note that time stamping is done at the beginning (start-bit) of every packet. In the ‘Source’- and ‘Destination’-column a slash separates the subnet from the node number or NID (e.g.: <subnet>/<node number>), groups are prelimited by a pound character (#<group>) and broadcasts are indicated by an asterisk (e.g.: <Subnet>/* or */*). Each packet that contains a protocol error of any kind (e.g.: CRC-error) is colored red in the packet table and the corresponding error is shown in the ‘Data’-column of the packet. For SNVT (Standard Network Variable Type) messages, the converted value is shown in the ‘Data’-column (instead of just the raw bytes). The SNVT of a network variable must be entered in the node editor of the packet converter (see Section 5.2) in order to make these conversions possible.

Packet Details

This area at the bottom of the log window displays more detailed packet information about the currently selected packet of the packet table. It shows general packet information, address and message information as well as the message (data) itself being transported in that packet. The packet message is shown in a listbox at the bottom of the packet detail area and displays the message in both numeric and textual (ASCII) form. Network management and diagnostic messages are interpreted according to the network protocol. Since message codes for application messages, network management messages and network diagnostic messages are overlapping, you have to choose the form of translation manually. Whenever this is the case, three buttons will appear at the bottom of the packet detail area where you can select how the current packet shall be interpreted (*Application*, *Management* or *Diagnostic*) as shown in Figure 26.

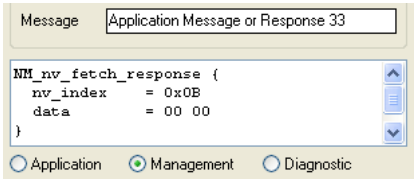


Figure 26: **Network Management and Diagnostic Messages**

Update messages of SNVTs (Standard Network Variables Types) are also interpreted and displayed correctly (see Figure 27). Like mentioned above, this is only possible when the network variable can be converted into a symbolic name due to the settings in the packet converter (see Section 5.2), and a SNVT is specified for that variable in the converter. When a SNVT message is shown, you can choose the type of display at the bottom of the packet detail area: ‘Raw’ means that no interpretation is done. ‘Structure’ means that the SNVT structure is shown but the values are not converted. ‘Converted’ means that the values contained in the SNVT structure are converted according to the SNVT Master List. Note that the measurement system can be switched between SI system and Imperial US system in the LPA Settings, see Section 5.11.

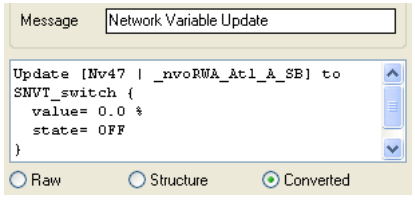


Figure 27: **SNVT Messages**

Protocol Details

This area is located under the packet table and shows protocol layer specific information of the currently selected packet. Each layer (PPDU, NPDU, TPDU, SPDU, AuthPDU and APDU) can be expanded to reveal information contained in that layer down to bit-level. At the bottom of the log window you can see raw packet data (hexadecimal) with a highlighted area which corresponds to the selected line of the protocol details.

Both packet details and protocol details can be switched on and off in the popup menu of the log window which appears when you click on the right mouse button.

4.4 Status Bar

This is the bar at the bottom of the LPA main window. It displays information about the currently active log or the last active log if no active log is present at the moment. Figure 28 shows the status bar of the LPA.

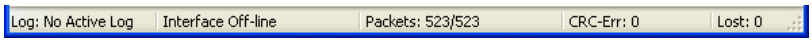


Figure 28: **Status Bar**

Log:

Here you can see the status of the active log. Possible values are: 'No Active Log' (no log is present at the moment), 'Not Running' (active log is present but packets are not being logged at the moment), 'Running On-line' (incoming packets are being logged and can be seen in the log window) and 'Running Off-line' (packets are being logged but the log window is not being updated at the moment). The log status changes whenever you select [menu Packet | Start Log], [menu Packet | Pause Update] or [menu Packet | Pause Log]. It is also influenced by the log mode settings (see Section 5.1).

Transceiver:

This is the field next to the 'Log:'-field. The transceiver selected in the interface settings is shown here, when a log is running. When no log is running, the message 'Interface Off-line' is displayed.

Packets:

Here you can see the number of packets that have passed the packet capture filter (see Section 5.3) and the number of all incoming packets in the form <captured>/<all>. This way you can always keep track of the actual number of logged and captured packets even if the packet statistics (see Section 5.5) are not shown or have been cleared at some point. The same goes for the number of CRC-errors described beneath.

CRC-Err:

The actual number of all packets with a CRC-error that have been received are shown here.

Lost:

The number of lost packets is displayed here (see Section 5.5).

4.5 Find and Go To Packet

In addition to scrolling through the packet table you can also search for a specific packet within a log window by selecting [menu Packet | Find...] or clicking on the button .

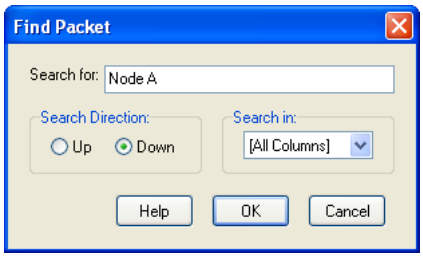


Figure 29: **Find Packet**

The dialog box for finding a packet is shown in Figure 29. It consists of the following panels:

Search for:

Here you can enter a sub-string of what you are searching for in the packet table of the active log window. Searching is not case-sensitive.

Search Direction:

The searching process always starts from the active (selected) line in the packet table. Here you can choose the search direction (up or down).

Search in:

Here you can select in which column of the packet table you want to search. Additionally you can choose to search in all columns.

When you click on 'OK', the first found packet will become the active line. You can search for the next line by hitting F3 or selecting [menu Packet | Find Next].

It is also possible to jump to a specific line number of the packet table by selecting [menu Packet | Go To...] or clicking on the button . Figure 30 shows the corresponding dialog box.

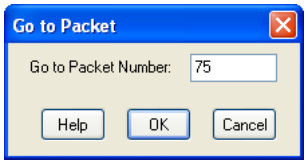


Figure 30: **Go To Packet**

4.6 Functions of the Popup Menu (View Menu)

The popup menu appears whenever you click on the right mouse button within a log window or select [menu View] as shown in Figure 31.

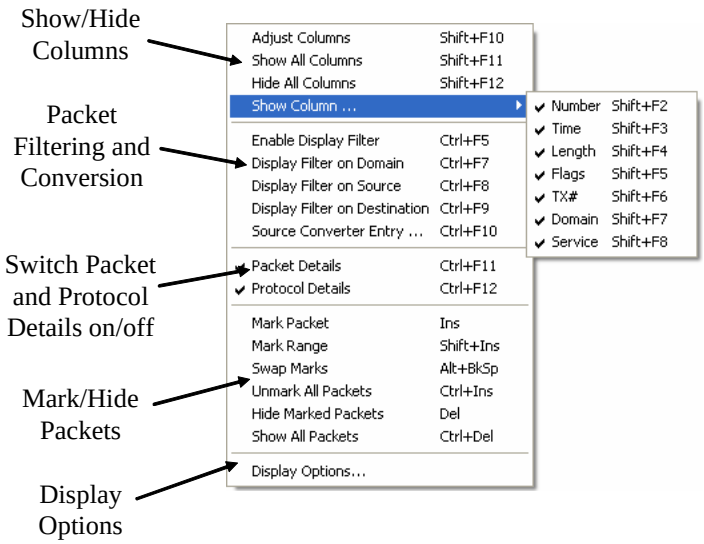


Figure 31: **Popup Menu (View Menu)**

Five major functions are provided by the popup menu:

Show/Hide Columns

Here you can choose which columns of the packet table and hence which information of each packet you wish to be visible. When you click on 'Hide all Columns' all columns except 'Source', 'Destination' and 'Data' will be hidden since these three are the most essential ones. By clicking on 'Adjust Columns', the width of all columns is adjusted to the currently displayed packet data.

Packet Filtering and Conversion

When clicking on 'Display Filter on Domain', a packet display filter is setup automatically that only shows packets from the domain of the currently selected packet. When clicking on 'Display Filter on Source', only packets that are transmitted or received by the source node are displayed. When clicking on 'Display Filter on Destination', only packets that are transmitted to or from the destination (node, subnet, or group) are displayed. To disable the display filter and show all packets again, 'Enable Display Filter' must be unchecked. The last used filter can be reactivated by checking 'Enable Display Filter'. By clicking on 'Source Converter Entry…' the packet converter for the selected source node is invoked. This can be used to change converter entries or setup new converter entries for unconverted nodes. For more information on packet filters and converters refer to Sections 5.2 and 5.3.

Switch Packet and Protocol Details on/off

Note that when both packet and protocol details are shown, they are displayed side by side at the bottom of the log window (see Figure 25).

Mark/Hide Packets

Here you can mark and unmark single packets as well as ranges of packets in the packet table. This is also possible by double-clicking on a packet (mark/unmark) or holding down the SHIFT-key while double-clicking on a packet (mark/unmark range). Marked packets can then be hidden if not interesting at a point. Marks can be canceled by choosing 'Unmark All Packets' and hidden packets can be shown again with 'Show All Packets'. You can always keep track of the number of marked and hidden packets by showing the packet statistics (see Section 5.5) for the current log. Note that marked packets are colored green in the packet table.

Display Options

Here you can invoke the Display Options dialog, see Section 5.4.

All functions of the popup menu can also be activated through the shortcut keys shown within the popup menu.

4.7 Logging Packets from the Network

To log packets from the connected network you have to create a new active log window first (button). After starting the logging process by selecting [menu Packet | Start Log | Network] or clicking on the button , incoming packets from the network are stored in the packet buffer. If you have enabled on-line mode (which is the default setting, see Section 5.1), you will be able to watch incoming captured packets in the log window. If on-line mode is disabled, you can only look at previously logged packets when the log is paused; while the log is running the log window will be blank. You can keep track of the number of total and captured packets in the packet statistics (see Section 5.5) or by watching the status bar.

4.8 Packet Log Files

A packet log file is created whenever you select [menu File | Save], click on the button or select [menu File | Save As...]. By default it has the extension '.plg'. The file contains all captured packets of that log, not only the ones that have passed the display filter (which are visible in the log window, see Section 5.3).

In addition to packet data the following information is stored in a packet log file:

- the path of the packet converter file if present (see Section 5.3),
- the path of the display filter file if present (see Section 5.3),
- the number of the currently active line in the packet table of the log window,
- the display options (see Section 5.4),
- the width and visibility of the packet table columns,
- the appearance of packet and protocol details in the log window,
- marked and hidden packets,
- the statistics trend (only in log files from LPA 3.0 or higher, see Section 5.8),
- some additional statistics values (only in log files from LPA 3.0 or higher),
- display options of the statistics window (only in log files from LPA 3.0 or higher).

Note that whenever you store an existing log file, these values will be rewritten. When you open a log file by selecting [menu File | Open...] or clicking on , the corresponding converter and filter files are opened if found in the stored paths. You can also use packet log files as a packet source for another log (like packet recording files, see Section 5.10).

Despite the new information in log files from LPA 3.0 (or higher), the log files stay both up- and downwards compatible. This means that a log file can be viewed with any LPA version regardless of the LPA version it was created with.

4.9 Exporting a Packet Log

You can export the packet table of the current log window as a CSV (comma separated value) file by selecting [menu File | Export...]. If you only want to export certain packets or columns use the display filter (see Section 5.3) and the popup menu functions of that log. In the first line of the exported file the names of the exported columns are stored. Lines (packets) are separated by new-line characters. The character used for separating columns as well as the decimal separator can be setup in the LPA Settings (see Section 5.11). The exported files can be used for further processing e.g. in spreadsheet programs.

4.10 Printing a Packet Log

You can print the packet table of the current log window by selecting [menu File | Print...]. You might want to reduce the number of displayed packets by using the display filter (see Section 5.3) and the hide-function of the popup menu before printing. In order to make packet information fit the paper's width you can use the hide-column-function of the popup menu. The dialog box for printing packets is shown in Figure 32.

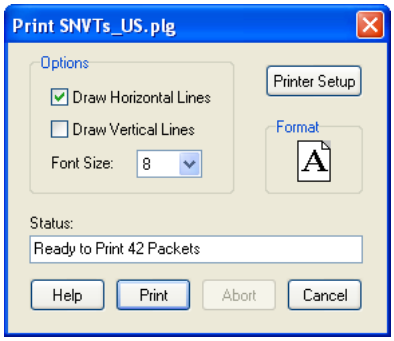


Figure 32: **Print Log**

Within the print form you can change the font size or choose landscape format (by clicking on 'Printer Setup'). Additionally you can choose to print horizontal and vertical lines. If the lines of the packet table do not fit on the paper, the message 'Packets will not fit on Paper' will appear and you will not be able to print. During the printing process you can watch the progress as well as abort.

4.11 On-line Help System

To invoke the on-line help system of the LPA, you have to select [menu Help | Help Topics]. If you click on the 'Help' button within a specific dialog box, context-sensitive help about the current form will appear. For general information on the LPA you can select [menu Help | About LPA...] and [menu Help | Contact...].

5 Advanced Features of the LPA

In addition to packet capturing and the display of packet information the LPA also offers more advanced features like packet filtering, conversion, statistics and simulation. The following sections describe the meaning of these terms and how the advanced functions of the LPA software are used.

5.1 Log Mode Settings

Before starting a packet log some settings concerning the mode of packet capturing and display can be done by selecting [menu Profile | Log Mode...] or clicking on the button LM. The corresponding dialog box is shown in Figure 33.

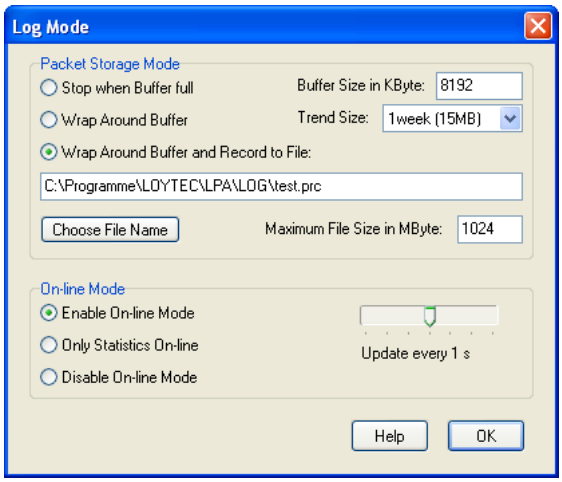


Figure 33: **Log Mode**

Packet Storage Mode

Here you can specify where to store incoming packets and how much memory shall be utilized as a packet buffer. Additionally the buffer size for the statistics trend (see Section 5.8) must be setup in the field 'Trend Size'. Three modes are available for packet storage: 'Stop when Buffer full' means that the logging process is stopped automatically when the packet buffer is full. In the 'Wrap around Buffer'-mode the oldest packets in memory are always overwritten by incoming new ones. The amount of main memory to be used as the packet buffer in Kbytes (up to 128 MB) can be selected at the top right corner of the dialog. In the third mode 'Wrap around Buffer and Record to File' you can additionally store all captured packets to a packet recording file. A packet recording file (*.prc) is a binary file which stores incoming packets during the logging process, see also Section 5.10. The maximum file size of the packet recording file in Mbytes (up to 16 GB) can be configured in the field 'Maximum File Size in Mbyte'.

On-line Mode

'Enable On-line Mode' means that you can watch incoming packets during the logging process. If your system cannot keep up to the speed of incoming packets you can try to 'Disable On-line Mode' or let just the packet statistics be updated while packets are logged ('Only Statistics On-line'). In on-line mode you can choose the update interval for the log window and statistics.

5.2 Packet Converter

Every log window has a packet converter assigned to it where symbolic names for network addresses and variables can be established to make packet contents easier to read and understand. These symbolic names are then displayed in the corresponding log window instead of the plain numbers contained in the packets. The conversion tables can be stored as packet converter files which have the extension '.pco' by default. Note that several log files can share the same converter file. If you change the converter within one of these logs, it will take effect on the other log files that use this converter file when they are opened again later. If you don't want that to happen, you must store the altered converter under a new name. Converter files can be merged by opening one file and clicking on 'Merge' for subsequent files. Observe also that you can setup a default converter in the LPA settings (see Section 5.11) which is used after start-up.

The packet converter of the current log window can be edited by selecting [menu Profile | Converter...] or clicking on the button . A small green point in the corner of the button indicates that converter entries are present (the converter is not empty) and the converter is active. You can activate and deactivate the converter by clicking on 'Enable Converter'. Additionally, you can invoke the packet converter for a specific domain, subnet, group, or node within the node statistics (see Section 5.6) or using the popup menu of the log table (Section 4.6). Please observe that you cannot cancel any modifications in the packet converter if you have disabled 'Backup Converter Settings' in the LPA Settings (see Section 5.11).

Figure 34 shows the dialog box for editing the packet converter. In all four tables of the converter you can delete a line by selecting the first column of that line and hitting DEL. You can insert a line the same way by pressing INS. All tables except the node table can be edited directly by pressing RETURN or clicking into a selected field of the table. You can clear all tables of the converter with the button 'Clear'.

Every line of the conversion tables starts with a symbolic name of the corresponding domain, subnet, group or node. Symbolic names have to start with a non-numeric character and can contain any character except ';', '=', '$', '#', '/' and '*'. There are four conversion tables: *Domains*, *Subnets*, *Groups* and *Nodes*.

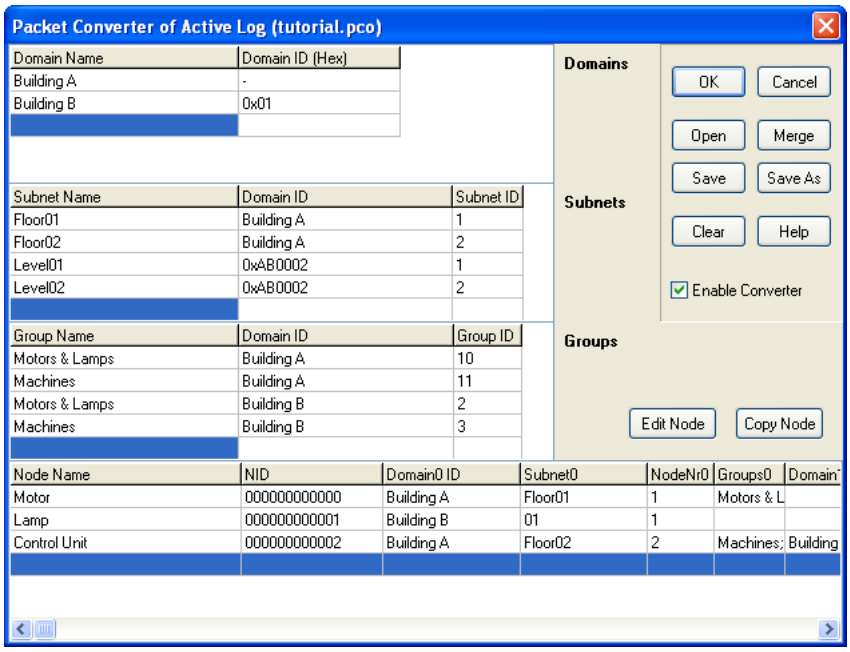


Figure 34: **Packet Converter**

Domains

Here you can assign symbolic domain names to domain IDs. Domain IDs must always be entered in hexadecimal form in one of the following formats according to the network protocol: 0xHH, 0xHHHHHH or 0xHHHHHHHHHHHH, where 'H' stand for a hexadecimal digit. In addition to that you can enter '--' to indicate the special domain with no ID (domain length = 0).

Subnets

In every row of the subnet table you can assign a symbolic subnet name to a subnet ID. You also have to specify the domain ID of every subnet. Subnet IDs can be entered in decimal (e.g.: 123) or hexadecimal form (e.g.: 0xAB). The domain ID can be entered as a symbolic domain name (defined in the domain table of the packet converter) or as a hexadecimal value as described above.

Groups

Here you can assign group names to group IDs in the same fashion. Group IDs can be entered in decimal (e.g.: 123) or hexadecimal form (e.g.: 0xAB) just like subnet IDs.

Nodes

This is the table at the bottom of the converter form. To edit a node you have to click on ‘Edit Node’ or double-click in the corresponding line of the node table. You can also copy an existing node by clicking on ‘Copy Node’. In both cases the node editor is invoked as shown in Figure 35.

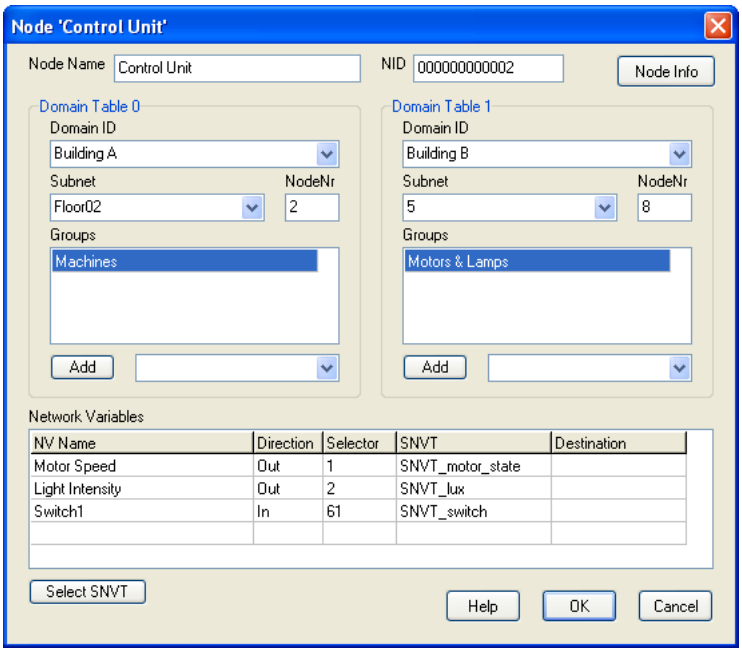


Figure 35: **Node Editor**

Node Name, NID and Node Info

Here you can edit the name of the node and its NID (Unique Node ID). NIDs must always be entered in hexadecimal form in the following format according to the network protocol: 0xHHHHHHHHHHHH, where ‘H’ stand for a hexadecimal digit. The prelimiter ‘0x’ is optional here. You can also enter the location and description of a node by clicking on the button ‘Node Info’. Note that this information is not processed during packet conversion and has no manifestation in the network protocol. It is only meant as a help for you to remember the purpose of that node. The value entered in the ‘Location’-field will appear in the header of the node editor.

Domain Tables

Every node can be a part of up to two domains which can be setup in the domain tables 0 and 1. If the node is unconfigured just leave all these entries blank. You can setup the domain ID, subnet and node number in each domain table. Additionally you can assign groups to the node by entering a group in the field next to the button ‘Add’ and then clicking on that button. The group will then appear in the table above. To delete a group from a domain table just click on the corresponding line and press DEL. Domains, subnets and groups can be entered as symbolic names (defined in the corresponding conversion tables) or as plain numbers in decimal or hexadecimal form.

Network Variables

Every line of this table represents a network variable of the node. It consists of the network variable’s name, direction and selector. Optionally you can also enter a SNVT and a destination address. The direction of a network variable specifies whether it is an input or output network variable. Possible values are ‘i’, ‘I’ or ‘In’ for input and ‘o’, ‘O’ or ‘Out’ for output. The selector identifies a network variable uniquely within the network. It can be

entered in decimal (e.g.: 12345) or hexadecimal form (e.g.: 0x0ABC). Entries of the network variable table can be edited directly by pressing RETURN or clicking into a selected field of the table. You can delete a network variable by selecting the 'NV Name'-column of the corresponding line and hitting DEL. You can insert a line the same way by pressing INS.

The SNVT (Standard Network Variable Type) is used to interpret network variable update messages of the corresponding network variable. Converted values of such messages are shown both in the packet table and the packet detail area of the log window. The SNVT can be entered directly (name or number). It can also be chosen from a list of available SNVTs by clicking on the button 'Select SNVT' (or double-clicking into the corresponding field) and selecting one of the available SNVTs. If you don't want to specify a SNVT for a network variable, just leave the 'SNVT'-field blank.

The 'Destination'-field is used to distinguish multiple outgoing network variables using the same selector. The destination address can be entered in one of the following formats:

- domain index:0/* ... network variable is broadcast domain-wide,
- domain index:subnet/* ... network variable is broadcast to the specified subnet,
- domain index:subnet/node no. ... network variable is sent to the specified node,
- domain index:#group ... network variable is sent to the specified group.

The domain index specifies one of the two domain entries in the current node. Possible values are 0 or 1. A value of '0:#lamps' e.g. would mean the group 'lamps' in the domain table entry 0 of the current node. Observe that apart from decimal or hexadecimal numbers also symbolic names from the packet converter can be used for subnets and groups. If you don't want to specify a destination address for a network variable, just leave the 'Destination'-field blank.

5.3 Packet Filters and the Packet Trigger

A packet filter decides whether to let a packet pass or reject it. It is used to reduce the amount of packets being analyzed. There are two types of packet filters, the capture filter and the display filter. During the logging process the capture filter decides whether to store a received packet or discard it. The display filter decides which of the captured packets are actually displayed in the log window. Note that you can automatically create a display filter for certain domains, subnets, nodes, and groups using the node statistics (see Section 5.6) or the popup menu of the log table (Section 4.6).

The capture filter is only present when an active log is present whereas every log window has a display filter assigned to it. Filter parameters can be stored as packet filter files which have the extension '.pft' by default. Note that several log files can share the same display filter file. If you change the display filter within one of these logs it will take effect on the other log files that use this packet filter file when they are opened again later. If you don't want that to happen, you must store the altered filter under a new name.

The packet filter form is also used for the packet trigger. This is a normal packet filter which decides when to start the capturing process. No packets are stored until a packet arrives which matches the packet trigger. After a packet has 'triggered' the logging process, the packet trigger is disabled and the capture filter starts to work instead. This trigger event is indicated by the disappearance of a small green point at the button

of the tool bar. After that you can re-activate the trigger by pausing the log and enabling the packet trigger again. Observe that you can setup default files for the capture filter, the

display filter and the trigger (in the LPA settings, see Section 5.11) which are used after start-up.

The capture filter of the active log can be edited by selecting [menu Profile | Capture Filter...] or clicking on the button CF. The display filter of the current log window can be edited by selecting [menu Profile | Display Filter...] or clicking on the button DF. A small green point in the corner of these buttons indicates that the corresponding filter is enabled. Figure 36 shows the dialog box for editing a packet filter.

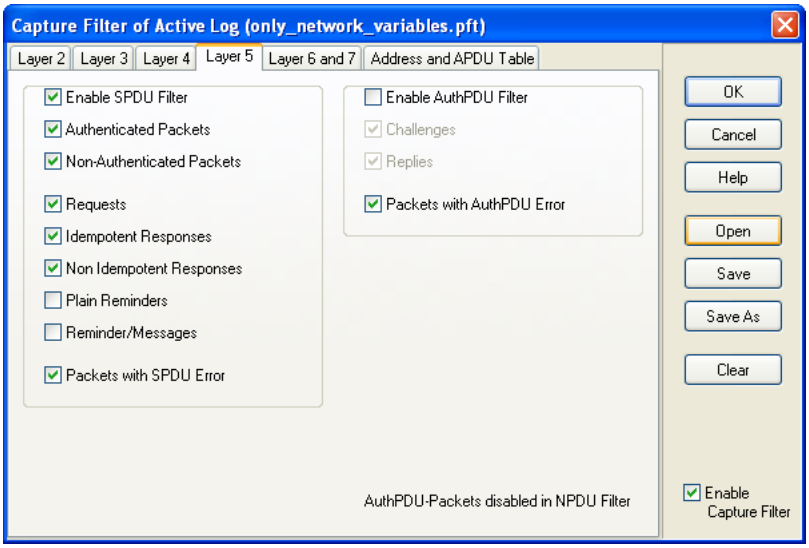


Figure 36: **Packet Filter**

A packet filter is divided into several sections corresponding to the layers (2-7) of the network protocol. Every section of the filter has a checkbox on top of the page where you can enable filtering on that layer. If a filter section is disabled no filtering is done on the corresponding protocol layer. It is also possible that parts of the filter are automatically disabled due to settings in lower layers. If that happens, a message is shown at the bottom of the disabled page. Figure 36 shows the filter section of layer 5 as an example. In this case the user has enabled the SPDU filter and has chosen to discard non-idempotent responses and plain reminders. For better performance during the packet logging process or if you want to see all captured packets, you can disable the whole packet filter with the 'Enable...'-checkbox at the right bottom of the filter form. With the button 'Clear' you can restore the default filter which discards all packets with protocol errors and lets all good packets pass.

Address and APDU Table

In addition to layer specific filter sections there is also the address and APDU table that provides packet sender, recipient, and message specific filtering. This is done separately because it is actually a combination of filtering on layer 3 (network addresses) and layer 6&7 (APDU). Figure 37 again shows the packet filter dialog box, this time displaying the 'Address and APDU Table'.

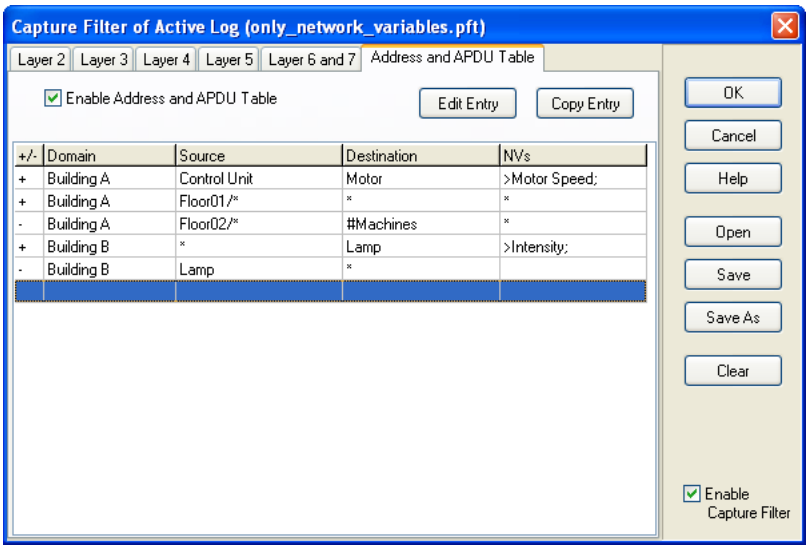


Figure 37: **Address and APDU Table**

In the first column of the table (‘+/-‘) a plus indicates a positive address entry whereas a minus indicates a negative address entry. Packets that match a positive address entry can pass the filter whereas packets that match a negative address entry are rejected. A packet has to match at least one positive address entry and is not allowed to match any of the negative entries in order to pass the filter. That is why there must always be at least one positive address entry, because no packet could pass otherwise.

Lines of the table can be deleted or inserted by pressing DEL or INS. You can edit an entry by clicking on ‘Edit Entry’ or double-clicking on the corresponding line of the table. You can also duplicate an existing entry by using the button ‘Copy Entry’. In both cases, the address editor of the packet filter is invoked as shown in Figure 38.

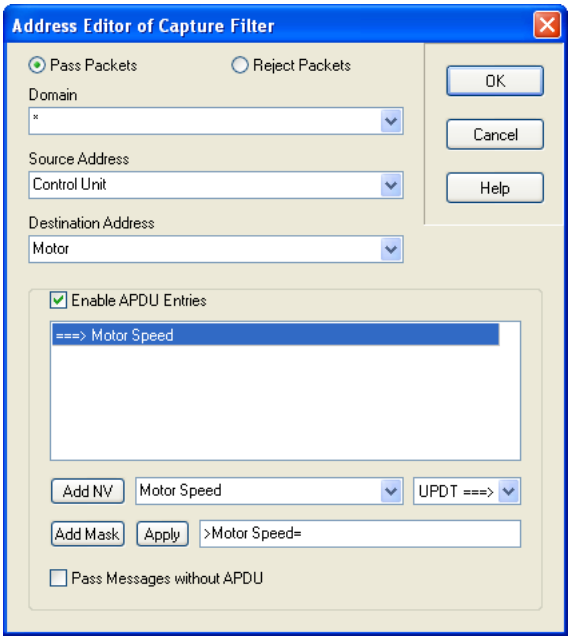


Figure 38: **Address Editor**

First you have to decide whether it shall be a positive or negative entry (‘Pass Packets’ or ‘Reject Packets’). In the ‘Domain’-field you can enter a symbolic domain name from the packet converter, a hexadecimal domain ID or an asterisk (‘*’) which means all domains.

The ‘Source Address’-field specifies the allowed sender(s) of the packet. It can be entered in one of the following formats:

- * ... source address is not checked,
- 0/0 ... sender is unconfigured,
- subnet/* ... all source addresses with that subnet,
- subnet/node number ... only packets with that source address,
- node name ... sender has to be that specific node.

The ‘Destination Address’-field specifies the allowed receiver(s) of the packet. It can be entered in one of the following formats:

- * ... destination address is not checked,
- 0/* ... all domain wide broadcasts,
- subnet/* ... all destination addresses with that subnet,
- subnet/node number ... only packets with that destination address,
- #group ... packets with that group as destination address,
- NID ... packets with that NID as destination address,
- node name ... that node has to be (one of) the receiver(s).

Note that apart from decimal or hexadecimal numbers also symbolic names from the packet converter can be used for subnets and groups. When you use a symbolic node name as the destination address, every packet that addresses that node will match this address entry regardless of the packet’s address format. Let’s say you specify the node ‘Lamp1’ in the packet converter with the NID 0x001122334455 in the domain 0x00 with subnet/node number 1/1 and the groups 0, 1 & 2. If you then enter ‘Lamp1’ as the destination address, every packet with the following characteristics will match that address entry:

- broadcasts in domain 0x00,
- broadcasts in subnet 1 of domain 0x00,
- packets with destination subnet / node number 1/1 in domain 0x00,
- packets with destination group 0, 1 or 2 in domain 0x00,
- packets with destination NID 0x001122334455.

If you have entered an asterisk (‘*’) in the ‘Domain’-field as described at the beginning, you can choose every node defined in the converter as the destination address (regardless of its domain table entries, which also includes unconfigured nodes). In this case only packets with NIDs as the destination address can match the address entry and therefore only the last point of the just given example would be true.

APDU Entries

In addition to the above you can specify a filter based on the APDU (application) part of the packets here. Several APDU entry types are available:

1. Filtering of network variables (polls, updates) without value match:

Just enter a network variable next to the 'Add NV'-button and then click on 'Add NV'. A network variable can be entered as a symbolic network variable name defined in a node of the packet converter as well as a selector in decimal (e.g.: 12345) or hexadecimal form (e.g.: 0x0ABC). You can also change the direction of the network variable message ('UPDaTe', 'POLL' or 'BOTH') beforehand.

2. Filtering of network variable updates with value match:

Enter a line of the following format into the field next to the 'Apply'-button:

- >network variable= value mask

and click on 'Add Mask'. All network variable updates of that network variable, where the updated value matches the mask, will match this entry. Bytes of the mask can be entered in hexadecimal (e.g.: '10 0A C7') or binary form (with a dot as an indicator, e.g.: '.00101011'). The wildcard character '?' can be used for ignoring certain nibbles or bits (e.g. '?5 ?? F?' or '.01?00??1').

3. Generic APDU filtering:

Just enter a data mask for the complete APDU in the field next to the 'Apply'-button and click on 'Add Mask'. A few examples are given below:

- 20 … all application msgs. with msg. code 0x20
- 20 12 .11110000 … all appl. msgs. with msg. code 0x20 and first data bytes = 0x12 0xF0
- 2? … all appl. msgs. with msg. codes 0x20 - 0x2F
- .1??????? .???????? … all network variable msgs. (two-byte msg. code, MSB=1)
- 6A … all query domain msgs. (network management code 0x6A)
- 40 ?? ?? … all foreign frame msgs. with msg. code 0x40 and at least 2 data bytes
- 10 .1??????? … all appl. msgs. with msg. code 0x10 and MSB=1 in the first data byte
- 10 ?? AB … all appl. msgs. with msg. code 0x10 and the 2. data byte = 0xAB

To edit an existing mask entry, click on the corresponding line, edit the mask and click on 'Apply'. To delete any APDU entry, just click on the corresponding line and press DEL. To let messages with no APDU (e.g. acknowledgements) match the address entry too, you must enable the checkbox at the bottom of the form.

5.4 Display Options

Every log window has display options assigned to it where the user can set how certain columns of the packet table shall look like. Display options of the current log window can be setup by selecting [menu View | Display Options...], clicking on the button , or using the popup menu (see Section 4.6). Figure 39 shows the corresponding dialog box.

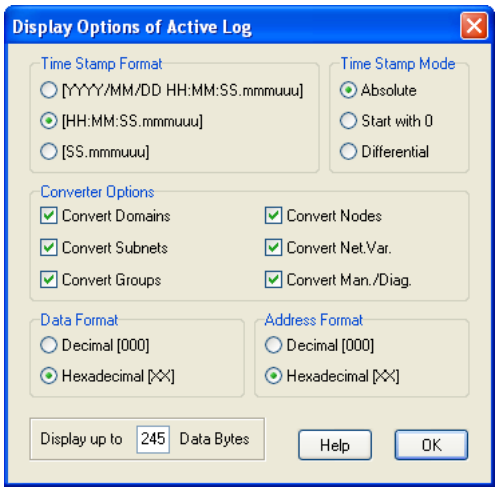


Figure 39: **Display Options**

Time Stamp Format

Here you can choose how detailed the time stamp of each packet shall appear.

Time Stamp Mode

Here you can choose between three modes of time stamp display. 'Absolute' means that the actual packet arrival time is displayed. 'Start with 0' means that the time between the first and the current packet is shown. If you choose 'Differential', the time between the current packet and the previous packet is displayed.

Converter Options

Here you can switch off conversion of domains, subnets, groups, nodes, network variables and management & diagnostic messages. Otherwise conversions (from plain numbers in the packet frame to symbolic names) are done automatically using the packet converter.

Data Format

Here you can select the format (decimal or hexadecimal) of message data shown in the packet table. This also affects the appearance of data presented in the protocol- and packet-details of the log window.

Address Format

Here you can select the format of unconverted address information (subnet ID, group ID, node number) in the columns 'Source' and 'Destination'. It also affects the appearance of addresses shown in the packet details. However, in the protocol detail area of the log window addresses are shown in both hexadecimal and decimal. Note that domain IDs and NIDs are always shown in hexadecimal form.

Display up to ... Data Bytes

Here you can enter the number of message data bytes (up to 245) that you wish to see in the column 'Data' of the packet table. If packets contain more data bytes, they will be truncated. However, in the protocol details of the log window you will be able to see all message data regardless of the settings done here.

5.5 Packet Statistics

The packet statistics provides statistical data of the current log window when you select [menu Packet | Statistics] or click on the button . The corresponding window is shown in Figure 40 (left picture). Statistics can also be displayed for the active log during the logging process if enabled in the log mode settings. In this case there is a 'Clear' button where you can reset all statistical data during packets are logged as shown in Figure 40 (right picture).

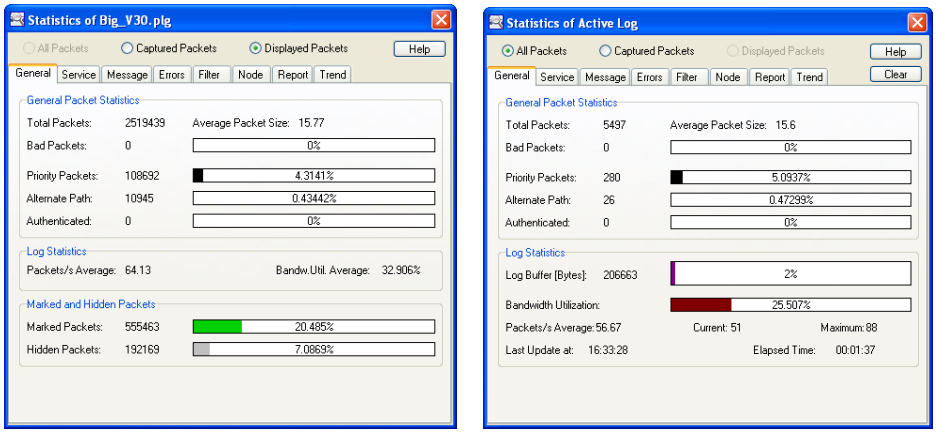


Figure 40: **Packet Statistics for Current Log Window and Active Log**

On top of the statistics window you can choose if you want to see the statistics of all packets or only the ones that have passed the packet filter. For the active log this means the capture filter, for all other log windows the display filter. That is why you can select 'All Packets' or 'Captured Packets' in the first case and 'Captured Packets' or 'Displayed Packets' in the second. Some other differences between statistics of a previously stored packet log file and statistics of the active log are described further beneath. Note that you can also keep track of the number of packets logged in the status bar. The packet statistics consists of several sections:

General

In the 'General Packet Statistics'-panel you can see the number of total packets and bad packets, average packet size and how many of the good packets are priority, alternate path or authenticated packets. At the bottom of the 'General'-section you can see either 'Log Statistics' (if statistics of active log) or both 'Log Statistics' and 'Marked and Hidden Packets' (otherwise). In the first case log buffer and bandwidth utilization as well as the average and maximum packet rate are displayed, in the second case the number of marked and hidden packets (see Section 4.6). The bandwidth utilization is calculated from the length of the packets (including preamble, start bit & code violation) as well as the average arbitration time of packets (β1-time, β2-time slots). A bandwidth utilization of 100% would mean that packets are sent continuously without any idle time on the network.

Service

Here you can see how many of the good packets are TPDU, SPDU, AuthPDU or unacknowledged packets (APDU only). For every of the mentioned PDU formats further classification relating to the service (PDU type) of the packets is done.

Message

In this section good packets are classified according to their message type (APDU type).

Errors

In the ‘Bad Packets’-panel you can see the number of bad packets (packets with protocol errors) on each layer of the network protocol including short packets and long packets. The reason for a short packet is either noise on the network or a collision during the transmission of the address field. The CRC error counter is incremented whenever a packet with an incorrect CRC is received. Reasons for CRC errors can again be noise or collisions (e.g. in the data field of the packet). All other counters in the ‘Bad Packets’-panel indicate invalid data in the packet sections belonging to layer 3-7 of the network protocol.

In the ‘Error Counters’-panel you can see the total number of detected errors, including errors not associated with received packets. A ‘Missed Preamble’ indicates a protocol error at the beginning of a packet. The ‘Interrupted Packets’ counter is incremented each time a packet is interrupted before the complete address information is successfully transmitted. This includes 'Short Packets', which are recorded in the LPA as well as packets that are too short to be stored as packets in the log (smaller than 2 bytes). The ‘Corrupted Packets’ counter is increased each time a corrupted packet (or part of a packet) is detected on the segment. This includes recorded packets with a CRC error as well as CRC errors in packets that are too small to be stored in the log. Possible reasons for the errors described above are: collisions (too many nodes try to send at the same time), poor cabling, too much noise on the channel, or interference from external devices.

Lost packets should not occur normally, since today’s PCs are fast enough to deal with the packet rates on CEA709 networks. However, if you get lost packets, you can try to go through the following steps to get better performance:

- close other applications,
- clear the packet converter,
- disable the packet filters (capture filter, display filter),
- change the log mode settings (disable on-line mode),
- disable the LPA Server and the LPA Plug-In in the LPA settings.

Filter

Here you can see how many packets have been filtered on each protocol layer. These values correspond to the capture filter if the statistics are shown for the active log. Otherwise the values correspond to the display filter.

The remaining statistics tabs ‘Node’, ‘Report’, and ‘Trend’ are described in the following Sections.

You can pause updates of packet statistics while the active log is running by selecting [menu Packet | Pause Update] or [menu Packet | Pause Log]. However, you can always force an update by clicking on one of the section headers (‘General’, ‘Service’, etc.).

5.6 Node Statistics

The node statistics provide domain, subnet, node, and group specific statistics when you select the ‘Node’ tab in the statistics window. The corresponding window is shown in Figure 41.

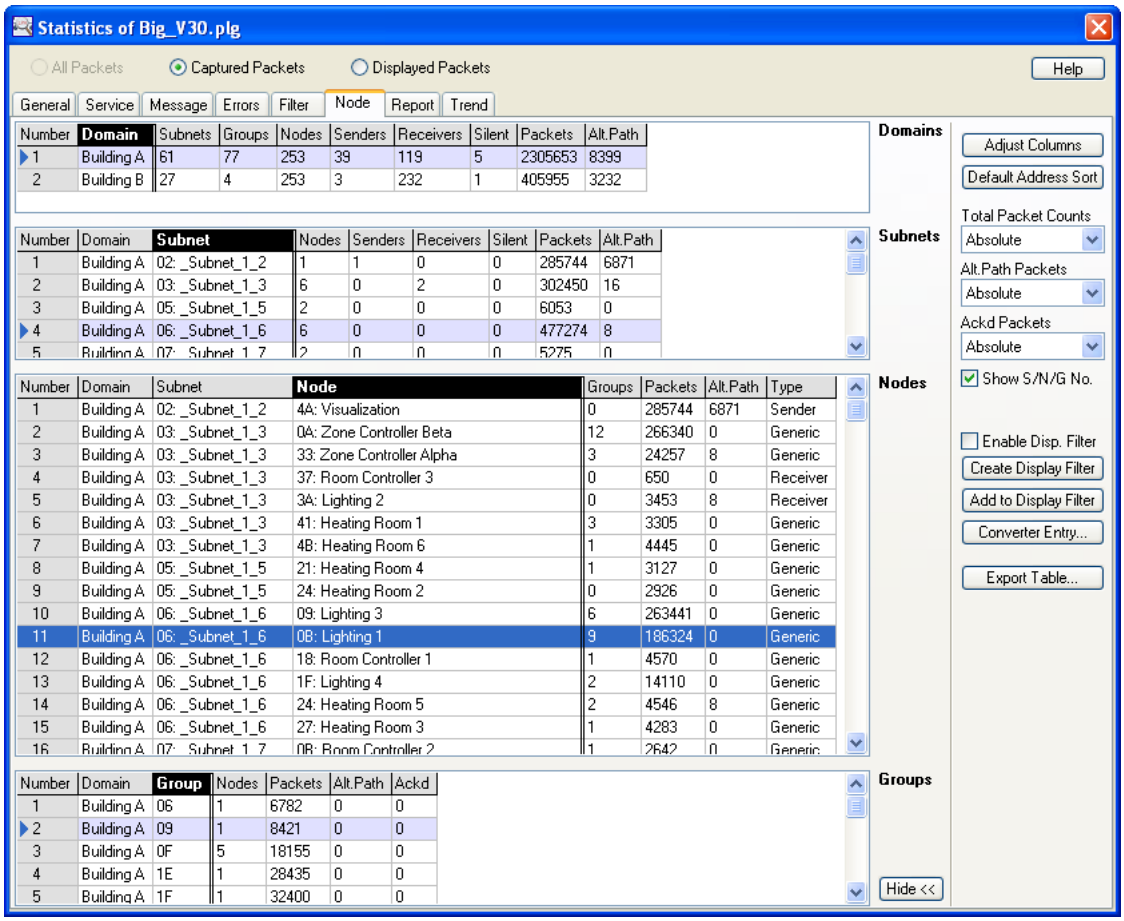


Figure 41: **Node Statistics**

All detected domains, subnets, nodes, and groups are shown in the four displayed tables. When clicking on a certain line in one of the tables, all corresponding lines in the other tables will be highlighted and small triangles will appear in the 'Number' column of these lines. In Figure 41 e.g. the selected node 'Lighting 1' resides in domain 'Building A', subnet '_Subnet_1_6' and is a member of group 0x09. Subnet, node, and group numbers are displayed in decimal or hexadecimal, according to the current display options of the observed log, see Section 5.4. The tables can be sorted by clicking on the column headers. Stacked sorting can be performed by clicking on several column headers starting with the least significant and ending on the most significant column to sort by. The width of each column can be adjusted to fit all contained cells by double clicking on the right border of the corresponding column header. Following is a description of all columns of the four tables:

Table 'Domains'
Column 'Domain': domain number or name (according to converter),
Columns 'Subnets', 'Groups', 'Nodes': number of subnets, groups, nodes in the domain,
Column 'Senders': number of nodes that primarily initiate transactions,
Column 'Receivers': number of nodes that primarily respond to initiated transactions,
Column 'Silent': number of detected nodes that have never transmitted a packet,
Column 'Packets': number of packets sent in this domain,
Column 'Alt.Path': number of alternate path packets sent in this domain.

Table 'Subnets'
Column 'Domain': domain the subnet resides in,
Column 'Subnet': subnet number and name (according to converter),
Column 'Nodes': number of nodes in the subnet,
Column 'Senders': number of nodes that primarily initiate transactions,
Column 'Receivers': number of nodes that primarily respond to initiated transactions,

Column ‘Silent’: number of detected nodes that have never transmitted a packet,
Column ‘Packets’: number of packets sent from this subnet,
Column ‘Alt.Path’: number of alternate path packets sent from this subnet.

Table ’Nodes’
Column ‘Domain’: domain the node resides in,
Column ‘Subnet’: subnet the node resides in,
Column ‘Node’: node number and name (according to converter),
Column ‘Groups’: number of groups the node was detected to be a member of,
Column ‘Packets’: number of packets sent from node,
Column ‘Alt.Path’: number of alternate path packets sent from node,
Column ‘Type’: Sender, Receiver, Generic (no specific transmission scheme), or Silent.

Table ’Groups’
Column ‘Domain’: domain the group resides in,
Column ‘Group’: group number and name (according to converter),
Column ‘Nodes’: number of nodes that have been detected to be a member of this group,
Column ‘Packets’: number of packets sent in this group,
Column ‘Alt.Path’: number of alternate path packets sent in this group,
Column ‘Ackd’: number of packets sent with acknowledged service.

Alternate path packets are sent out if the destination node does not answer to requests or acknowledged packets. The number of alternate path packets - shown in all four tables - is therefore an indicator for problems of (a) destination node(s). Silent nodes should also be investigated to check why the nodes are addressed but never send a packet on the observed network segment. The number of acknowledged packets in groups (last column) is displayed because the acknowledged service can lead to problems in large groups. More detailed information about detected problems can be found in the LPA report, see Section 5.7.

The panel on the right side of the node statistics window offers the following options and functions:

Adjust Columns

This adjusts the width of all columns to fit the contained table cells.

Default Address Sort

Sorts all tables hierarchically by address (e.g. domain / subnet / node in case of node table).

Total Packet Counts

Sets the display mode for the ‘Packets’ columns of all four tables. ‘Absolute’ shows the absolute packet count, ‘% of Traffic’ shows the percentage of packets based on total traffic, ‘Average Rate’ shows the average packet rate, and ‘Current Rate’ shows the current packet rate (only available on-line).

Alt.Path Packets

Sets the display mode for the ‘Alt.Path’ columns of all four tables. ‘Absolute’ shows the absolute count of alternate path packets, ‘% of Total’ shows the percentage of alternate path packets based on the total number of packets of the domain, subnet, node, or group.

Ackd Packets

Sets the display mode for the ‘Ackd’ column of the group table. ‘Absolute’ shows the absolute count of packets with acknowledged service, ‘% of Total’ shows the percentage of these packets based on the total number of packets of the group.

Show S/N/G No.

If this checkbox is enabled, the subnet, node, and group numbers are always displayed in the corresponding columns even if symbolic names are available from the packet converter, e.g. see columns ‘Subnet’ and ‘Node’ in the node table of Figure 41. If the checkbox is disabled, numbers are only displayed if no conversion is available. Observe that in this case, the corresponding columns are sorted by name only.

Enable Disp. Filter

This checkbox can be used to quickly disable any display filter that was created automatically through one of the following two functions:

Create Display Filter

Click this button to create a display filter for the observed log, which only displays packets of the currently selected domain, subnet, node, or group. When a node is selected, all packets sent *and received* by that node are shown, as long as they can be assigned to the node.

Add to Display Filter

Click this button to add the currently selected domain, subnet, node, or group to an already existing display filter. This way, e.g. the traffic of several nodes can be displayed.

Converter Entry…

Click this button to add or modify the packet converter entry of the currently selected domain, subnet, node, or group.

Export Table…

Click this button to export the currently selected table to a CSV (comma separated value) file. Separator characters can be setup in the LPA Settings (Section 5.11).

Note that the last five functions are also available through the popup menu of the domain, subnet, node, and group table, see Figure 42.

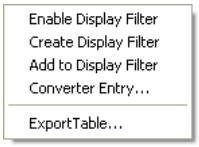


Figure 42: **Popup Menu of Node Statistics**

5.7 LPA Reports

LPA Reports offer a quick overview of the observed network segment. The report tab of the statistics window is shown in Figure 43.

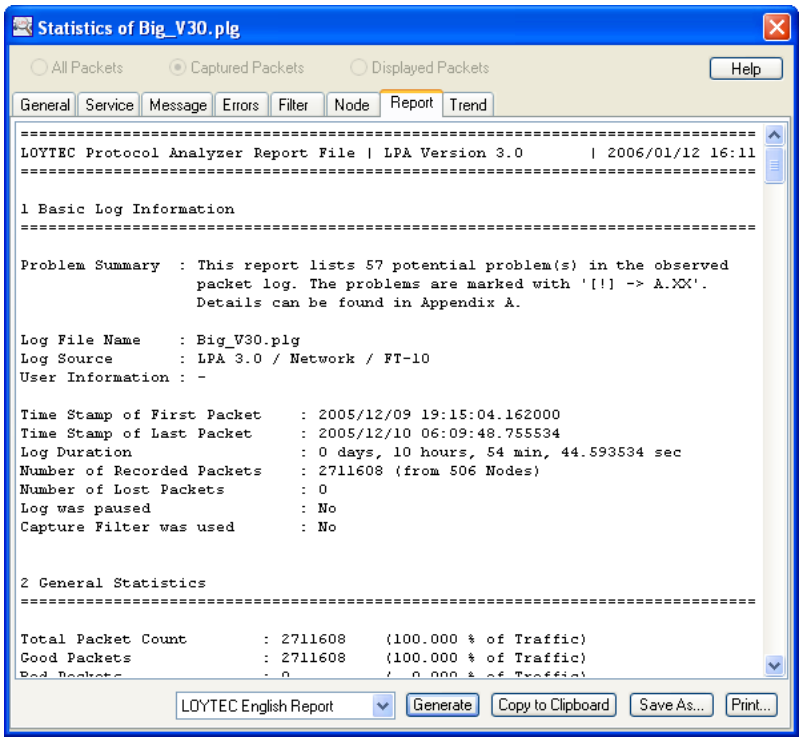

Statistics of Big_V30.plg
All Packets
Captured Packets
Displayed Packets
Help
General
Service
Message
Errors
Filter
Node
Report
Trend
LOYTEC Protocol Analyzer Report File | LPA Version 3.0 | 2006/01/12 16:11
1 Basic Log Information
Problem Summary : This report lists 57 potential problem(s) in the observed packet log. The problems are marked with '[!] -> A.XX'. Details can be found in Appendix A.
Log File Name : Big_V30.plg
Log Source : LPA 3.0 / Network / FT-10
User Information : -
Time Stamp of First Packet : 2005/12/09 19:15:04.162000
Time Stamp of Last Packet : 2005/12/10 06:09:48.755534
Log Duration : 0 days, 10 hours, 54 min, 44.593534 sec
Number of Recorded Packets : 2711608 (from 506 Nodes)
Number of Lost Packets : 0
Log was paused : No
Capture Filter was used : No
2 General Statistics
Total Packet Count : 2711608 (100.000 % of Traffic)
Good Packets : 2711608 (100.000 % of Traffic)
LOYTEC English Report
Generate
Copy to Clipboard
Save As...
Print...

Figure 43: **LPA Report**

At the bottom of the window a report type can be selected before generating the report by clicking on ‘Generate’. Custom report types can be programmed, as described in Section 6.4. The report can be copied to the clipboard and pasted to a different application. It can also be saved (‘Save As…’) and printed (‘Print…’). The report files generated with LOYTEC report types consist of the following sections:

1 Basic Log Information

Contains some basic information about the observed log and provides a brief problem summary.

2 General Statistics

Shows general packet statistics corresponding to the different protocol layers.

3 Error Statistics

Contains the most important bad packet counters and error counters including a brief description.

4 Domain Statistics

Provides basic statistics of all detected domains. The domains are sorted according to the sort mode of the node statistics.

5 Potential Node Problems

Lists all potential node problems such as alternate path packets or silent nodes. The nodes are sorted according to the sort mode of the node statistics.

6 Potential Group Problems

Lists all potential group problems. The groups are sorted according to the sort mode of the node statistics.

A Appendix

Provides a detailed description of all detected problems including hints for solving the problems.

5.8 Statistics Trends

In the ‘Trend’-tab of the statistics window, the trend of the bandwidth utilization as well as the missed preamble and corrupted packet counter is displayed, as depicted in Figure 44.

Figure 44: **Statistics Trends**

Observe that the trend is only available for packet logs generated with LPA Version 3.0 or higher. You can zoom into the trend by left-clicking into one of the two charts. Zooming out is performed by holding the ‘CTRL’-key while left-clicking. You can also pan around in the trend by right clicking into a chart and dragging it to the left or right. The panel on the right side of the trend window provides the following functions:

Zoom Listbox (at the top of the panel)

Here you can choose between different zoom levels: ‘Show All’ fits the complete trend into the charts. ‘Zoom and Pan’ allows you to zoom and pan manually as described above. All other settings show a certain section of the latest part of the trend. This is useful for on-line observation, since in this case the charts automatically scroll to the left as soon as new values arrive.

Go to Packet (only available off-line)

By clicking on this button, the packet at the beginning of the displayed range is selected in the packet log. The position of the currently selected packet is always indicated as a blue bar in the charts of the trend as shown in Figure 44.

Export Trends…(only available off-line)

Click this button to export all trend values to a CSV (comma separated value) file. Separator characters can be setup in the LPA Settings (Section 5.11).

5.9 Packet Simulation

To learn about the functions of the LPA and the network protocol in general, you can simulate packets as if they were coming from a real network. Every possible packet can be created from data you input. All functions of the analyzer like filtering, conversion and statistics can be utilized during packet simulation. After you have created a new active log window and setup the log mode you can start packet simulation by selecting [menu Packet | Start Log | Simulate]. A dialog box will appear as shown in Figure 45.

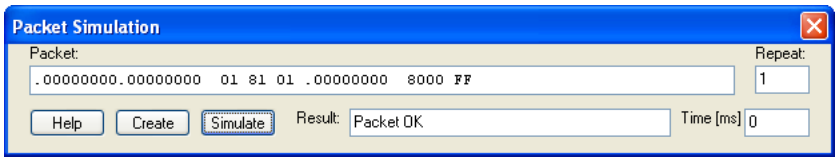


Figure 45: **Packet Simulation**

Here you can simulate packets as if they were coming from the network. You can enter the raw packet you want to simulate in the field ‘Packet:’. Note that the CRC is calculated automatically and therefore does not have to be input. Bytes of the packet can be entered in hexadecimal (e.g.: ‘FF 0A C7’) or binary form (with a dot as an indicator, e.g.: ‘.00101011’). You can also choose to send the packet several times as fast as possible in the field ‘Repeat:’. After simulating the packet(s) by clicking on the button ‘Simulate’ you will get a ‘Result:’-message which tells you if the packet has protocol errors and if it has been filtered by the capture filter or display filter. In addition to that the time it took to log the packet(s) is also displayed, which gives you a rough estimation of your system performance. If you don’t want to bother with the bits and bytes of the network protocol, you can also create a packet by clicking on the button ‘Create’ which invokes the dialog box shown in Figure 46.

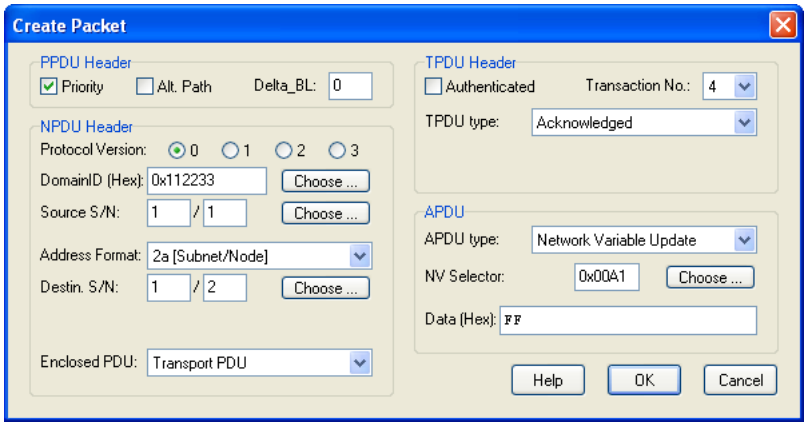


Figure 46: **Packet Creation**

Here you can enter all parameters required to create a packet. That starts with layer 2 (first byte of packet) and ends on layer 6&7 of the network protocol. This way you can also learn more about the various formats of network packets. Note that only good packets (without protocol errors) can be created here; if you want to simulate bad packets (which contain protocol errors) you have to edit them manually in the packet simulator. The ‘Create Packet’-window consists of the following panels:

PPDU Header

This represents layer 2 of the network protocol. Here you can set the priority and alternate path flag as well as the channel backlog increment (‘Delta_BL’).

NPDU Header

The Network PDU (Protocol Data Unit) represents layer 3 of the network protocol. You can setup the protocol version, address information and the enclosed PDU format here. The domain ID as well as source subnet and node number have to be entered. For the destination address you have to choose one of the possible address formats first. Depending on that format you will have to enter destination subnet, node number, group or NID. When you want to use address format 2b, you will additionally have to enter source group and member. You can also let the address information be set automatically by choosing symbolic names defined in the packet converter (click on the corresponding ‘Choose…’ button).

TPDU, SPDU or AuthPDU Header

This is the section at the upper right corner of the form. Depending on settings in the NPDU header (‘Enclosed PDU’) one of these three panels will appear. They represent layer 4 or 5 of the network protocol. You can set the authentication flag and transaction number of the packet here. Each of the three possible headers (TPDU, SPDU or AuthPDU) provides several services which can be chosen in the field ‘...PDU type:’. Some of these services require additional information which has to be entered at the bottom of the panel in hexadecimal form (member list, random bytes, crypto bytes).

APDU

The APDU panel appears whenever a message (Application Protocol Data Unit) can be transported in the packet. This is not the case with acknowledgments, plain reminders, challenges and replies. In all other cases you will first have to set the APDU type. If you select ‘Network Variable Update’ or ‘Network Variable Poll’ you will have to enter the corresponding network variable selector (‘NV selector:’). In all other cases you must enter the message code (‘... Code:’). The selector- or code-field can also be set automatically by choosing a symbolic network variable name or a message name (button ‘Choose…’). If you don’t want any message to be transported in the packet you have to select ‘APDU with Length 0’. Otherwise you can then enter additional data in hexadecimal form at the bottom of the panel, e.g. a network variable update value.

When you click on ‘OK’, the packet will be created and written to the ‘Packet:’-field in the simulation dialog box (see Figure 45).

5.10 Packet Recording Files

Packet recording files are binary files that store packet data on-line during the logging process. They have the extension ‘.prc’ by default. To create a packet recording file you have to select ‘Wrap Around Buffer and Record to File:’ in the log mode settings [menu Profile | Log Mode] and then start the log [menu Packet | Start Log]. All captured packets are then written directly to the packet recording file. The advantage of packet recording files over normal packet log files is that you can record packets until virtually all harddisc space is utilized (up to 16 GB), whereas packet log files can only store the packets that are located in main memory (up to 128 MB). The disadvantage is that you cannot open a packet recording file directly, you have to start a new log from file instead.

Packets can be logged from packet recording files in two modes: normal mode [menu Packet | Start Log | from File...] and trace mode [menu Packet | Start Log | from File (trace)...]. In normal mode packets are logged as fast as possible from the packet recording

file and time stamps remain the same. If you start the log in trace mode, packets are simulated as if they were coming from the network, one packet every other second. The time stamp of each packet is reset to the actual time when that packet arrives in the packet buffer. This way packet recording files can be used not only for long time event-recording but also to demonstrate functions of the LPA and the network protocol (also see Chapter 3). Note that in trace mode you can use all features of the LPA software, just as if packets would come from the network.

To provide flexibility between packet log files and packet recording files, a standard packet log file can be used to log packets from too. It is also possible to log packets *from* a packet recording file *to* another one. This is useful when the file size shall be reduced by filtering out unwanted packets (with the capture filter). To sum it up it can be said that the packet source of a log (network, simulation or file) is independent of the log mode settings where it is decided how to store packets (packet buffer, packet recording file). Note that all packets that have been logged to the packet buffer can be stored to a packet log file after the logging process has been stopped.

To split huge packet recording files into smaller parts that can be logged entirely and stored to a packet log file without packet loss, a function called 'Split PRC Files' has been established. It is activated by selecting [menu File | Split PRC Files...]. The size of the resulting files can be setup in the LPA settings (see Section 5.11). The names of the files will be composed of the original file name and a number. The file 'test.prc' e.g. will be split into the files 'test0000.prc', 'test0001.prc', etc. Please be patient when you select this function since it takes a while to process large files. When all files have been written, a message will appear showing the number of created files. Observe that the original packet recording file is not deleted.

5.11 LPA Settings

General settings of the LPA can be changed by selecting [menu File | Settings...]. By clicking on 'Default' you can restore the previous settings. When you click on 'Save as Default', the currently shown settings are stored as the default. Settings will also be stored automatically upon exiting the LPA. Figure 47 shows the 'LPA Settings'-window.

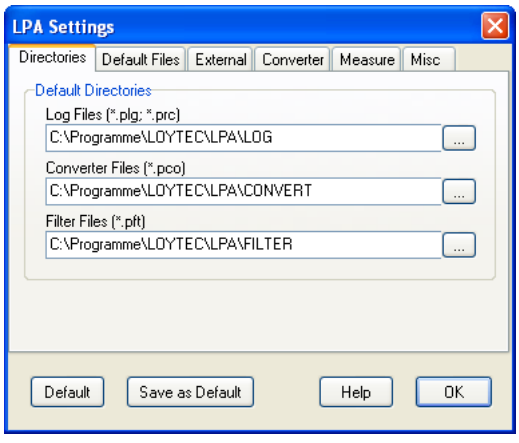


Figure 47: **LPA Settings**

On top of the LPA settings form the following sections are available:

Directories

Here you can setup default paths for Log Files (normal log files and packet recording files), packet converter files and packet filter files.

Default Files

Here you can setup default files for the packet filters (trigger, capture filter & display filter) and the packet converter. These files will be used for new packet logs after start-up of the LPA. If you don't want a default file to be used, just click on the button 'Clear'.

External

Here you can activate the LPA Server as well as choose an LPA Plug-In. The LPA Server forwards all received packets that pass through the capture filter to external programs (LPA Clients). An LPA Plug-In is an external DLL (Dynamic Link Library) which can change the interpretation and hence the display of packets. See Chapter 6 for more information on how to create LPA Clients and Plug-Ins. Observe that using the LPA Server or an LPA Plug-In can slow down the logging process.

Converter

Here you make some settings for the packet converter. By choosing 'Prompt before deleting Domains, Subnets or Groups' you will be asked for confirmation before you delete domains, subnets or groups which names are already used in other tables of the packet converter or the packet filters. The same goes for 'Prompt before deleting nodes'. 'Prompt before changing corresponding Entries' means that whenever you change the name of a domain, subnet, group, node or network variable which is already in use somewhere else, you will be asked if these corresponding entries should be changed too. Otherwise the changes are done without prompting. If you disable 'Backup Converter Settings', the processing of large converter files will be significantly faster, but you will not be able to cancel any manual changes in the converter dialog. This option was introduced to make possible the use of very large converter files e.g. derived from an LNS database using the LPAConv utility.

Measure

In the 'Measurement System'-panel you can choose between SI system and US (Imperial) System for the display of SNVTs. In US system, additional display options are available, which can be setup in the remaining fields. Observe that these options only apply to SNVTs where multiple formats are available.

Misc

In the 'Time Stamp Settings'-field you can choose to synchronize the hardware packet time stamps from the network interface to your PC's local system time. This is useful when running other applications in parallel that also display the PC system time and matching time stamps are required. Observe that using this option will decrease the relative accuracy of the time stamping to about 10µs (instead of 1µs). In the 'Packet Recording Files'-field you can setup the size of the files which shall be created when a packet recording file is split into smaller parts. The size must be entered in MBytes (up to 64 MB). In the 'Export Settings'-field you can setup the separator characters for exported CSV (comma separated value) files. By default, the separator characters are derived from the Windows local settings.

6 External Applications

This chapter describes how the LPA software can be used with external applications. It is shown how packet recording files are accessed, how packets can be forwarded to third party software and how the LPA can be customized to display application specific data. Sample programs (in the language C) are included with the LPA software in the subdirectory 'SOURCE' of your LPA installation folder.

6.1 Accessing Data from Packet Recording Files

Since packet recording files (see Section 5.10) have a rather simple format, it is easy to read the packet data they contain. Basically the file must be opened in binary mode, the file header must be skipped and then the packets can be read until the end of the file is reached. Each packet consists of a length information (two bytes), the packet itself (from priority bit to CRC) and a timestamp. The exact procedure is shown in the example 'ProcPRC' which is located in the folder 'SOURCE\ProcPRC' of your LPA installation directory. The file 'ProcPRC.c' contains all the source code needed for the example. The file 'ProcPRC.sln' (in the same folder) is a solution file for Visual C++® 7.1. There is also a compiled executable file available located in the folder 'SOURCE\ProcPRC\Release' called 'ProcPRC.exe'. It reads the packet recording file 'test.prc' and displays packet data in a console window.

6.2 LPA Server and Clients

The LPA can forward information to third party applications while packets are logged. This feature is activated by starting the LPA Server (see Section 5.11). The LPA Server automatically writes all packets that pass through the capture filter (see 5.3) into a packet ring-buffer that can store up to 128 packets. So called LPA Clients can access packet data on-line by using the DLL 'LpaCli.dll'. This DLL provides two functions to read packet data and wait for new packets. To avoid blocking of the LPA software while packets are logged, there is no hand-shaking between the server and the clients. This means that the clients must process packet data fast enough in order not to lose any packets. Other than that there is no limitation on the number of clients running at the same time. It is also possible to start and stop the LPA Clients as well as the LPA Server at any time, the synchronization is always done automatically. To create an LPA Client application, the DLL (Dynamic Link Library) 'LpaCli.dll', which is located in the folder 'SOURCE\LpaCliT\Release' of your LPA installation directory, must be linked to your application. The example 'LpaCliT' in the folder 'SOURCE\LpaCliT' shows how to use the DLL. It is a simple application that receives all packets from the LPA Server and displays them in the console-window. The file 'LpaCliT.c' contains the source code of the example. In the file 'LpaCli.h', which is included in 'LpaCliT.c', the two functions of the DLL 'LpaCli.dll' are declared:

```
DWORD LpaCliWaitForPacket(    //wait for packet from LPA server
  DWORD TimeOut               //timeout in ms (or INFINITE to wait infinitely)
);
```

The `LpaCliWaitForPacket` function suspends the calling program (LPA Client) until a new packet is received from the LPA Server or the timeout-value `TimeOut` is exceeded. To wait infinitely `TimeOut` has to be set to `INFINITE`. The function returns `LPACLI_OK` if a new packet has arrived and `LPACLI_TIMEOUT` when the `TimeOut` has occurred. If a fatal error has occured, the function returns `LPACLI_COULD_NOT_START`.

```
DWORD LpaCliReadPacket(       //get next packet from LPA server
  LpaPacket_t *LpaPacket      //buffer that receives packet from LPA server
);
```

The `LpaCliReadPacket` function reads the next packet from the LPA Server ring-buffer. The parameter `LpaPacket` must point to a structure of the type `LpaPacket_t` which is defined in 'LpaPFmt.h'. If a packet can be read, this structure receives the packet data and the `LpaCliReadPacket` function returns `LPACLI_OK`. If there is no packet in the queue, the function returns `LPACLI_NO_PACKET`. If a fatal error has occurred, the function returns `LPACLI_COULD_NOT_START`. From the file 'LpaPFmt.h' (which is included in 'LpaCli.h') only the declaration of `LpaPacket_t` is needed for LPA Clients. The other declarations are required for LPA Plug-Ins only (see Section 6.3). The type of the `LpaPacket_t` structure is declared as follows ('LpaPFmt.h'):

```
typedef struct _LpaPacket_t           //LPA packet information
{
  //textual packet information
  char AbsoluteTime[32];      //absolute time stamp
  char ColLength[10];         //column 'Length'       in LPA packet table
  char ColFlags[16];          //column 'Flags'        in LPA packet table
  char ColTXNo[8];            //column 'TX#'          in LPA packet table
  char ColDomain[33];         //column 'Domain'       in LPA packet table
  char ColSource[128];        //column 'Source'       in LPA packet table
  char ColDestination[128];   //column 'Destination'  in LPA packet table
  char ColService[16];        //column 'Service'      in LPA packet table
  char ColData[1024];         //column 'Data'         in LPA packet table

  //numeric packet data
  BYTE RawPacket[8192];       //raw packet from priority bit to CRC
  DWORD Length;               //length of packet from first byte to CRC
  DWORD MessageStart;         //start of APDU (0 if no APDU)

  //additional packet information
  DWORD PacketId;             //packet ID
  DWORD PreambleLength;       //number of preamble bits before packet
  LONG TimeStampSec;          //seconds of packet timestamp
  LONG TimeStampNanoSec;      //nano seconds of packet timestamp
  DWORD Error;                //greater than 0 if packet has errors
}LpaPacket_t;
```

The textual packet information simply consists of the columns of the corresponding line in the LPA packet table (see Section 4.3). Exceptions are the column 'Number' (which is not returned) and the value `AbsoluteTime`, which always returns the full, absolute time stamp regardless of the settings in the LPA display options (see 5.4). Numeric packet data includes the `RawPacket` which contains the whole packet from priority bit to CRC. The length of the packet (in bytes) is returned in `Length` and the index of the first byte of the APDU (Application Protocol Data Unit) is returned in `MessageStart`. Observe that `MessageStart=0` means that the packet contains no APDU (e.g. acknowledgement packets). Additional packet information includes the `PreambleLength` of the packet, the timestamp, the `Error` flag and a `PacketId`. The `TimeStampSec` value can be split into date and time by using the `localtime` function as shown in the 'ProcPRC' example ('SOURCE\ProcPRC\ProcPRC.c'). The `PacketId` starts with 0 when the LPA Server is activated and is incremented by the server whenever a new packet is written. It can be used in the client to determine if packets have been lost.

The 'LpaCliT' example includes a Visual C++ 7.1 solution file called 'LpaCliT.sln'. The following settings have been made in the Visual C++ Developer Studio: In [menu Project | Properties | C/C++ | Code Generation] the 'Struct Member Alignment' is set to 1 Byte. This is necessary for working correctly with the LPA Client DLL. In [menu Project | Properties | Linker] the value 'LpaCli.lib' has been appended to the 'Additional Dependencies'. The corresponding library file 'LpaCli.lib' is located in the folder 'SOURCE\LpaCliT' of your LPA installation directory. A compiled executable file ('LpaCliT.exe') is located in

'SOURCE\LpaCliT\Release'. When both this file and the LPA Server is started, all logged packets can be watched in the console-window of 'LpaCliT.exe'. Observe that the client ('LpaCliT.exe') can be started multiple times like mentioned above.

6.3 LPA Plug-Ins

The display of packet information in the LPA can be customized by creating an LPA Plug-In and activating it in the LPA settings (see Section 5.11). This is useful for specific interpretation of user and application data (user defined network variables, explicit messages, foreign frames, etc). An LPA Plug-In is a DLL (Dynamic Link Library) which is used by the LPA whenever packet data shall be displayed. The DLL must provide the following two functions:

```
BOOL LpaPlgChangePacket(        //change packet display in LPA packet table
  LpaDisplayOptions_t *LpaDisplayOptions,     //current LPA display options
  LpaPacket_t *LpaPacket        //packet to be displayed in packet table
)
```

The `LpaPlgChangePacket` function is called by the LPA right before a packet shall be displayed in the packet table. The packet information is passed in the parameter `LpaPacket`. It has the same format as the structure used for LPA Clients (see Section 6.2). The textual information contained in this structure is about to be displayed in the packet table. In the function `LpaPlgChangePacket` it has to be decided, if this information shall be changed before output on screen. The values `ColDomain`, `ColSource`, `ColDestination` and `ColData` (and hence the columns 'Domain', 'Source', Destination' and 'Data') can be changed by overwriting the corresponding members of the structure `LpaPacket`. If the values have been overwritten, the `LpaPlgChangePacket` function must return `TRUE`. If the packet has not been changed the function must return `FALSE`. The parameter `LpaDisplayOptions` contains the current settings of the LPA display options dialog (see 5.4). This can be used e.g. to format integer values according to the current user settings (decimal or hexadecimal).

```
BOOL LpaPlgChangePacketDetails( //change display of LPA packet details
  LpaDisplayOptions_t *LpaDisplayOptions,     //current LPA display options
  LpaPacket_t *LpaPacket,       //packet to be displayed in detail
  LpaPacketDetails_t *LpaPacketDetails  //buffer that receives packet details
)
```

The `LpaPlgChangePacketDetails` function is called by the LPA right before a packet shall be displayed in the packet detail area of the log window (see Section 4.3). Like in the previous function, the parameter `LpaPacket` is passed to decide if the packet information shall be changed before output. The parameter `LpaDisplayOptions` has also the same meaning as for the `LpaChangePacket` function. Additionally the `LpaPacketDetails` parameter points to a structure containing the textual information that is about to be displayed in the packet detail area. The format of this structure is shown here (file 'LpaPFmt.h'):

```
typedef struct _LpaPacketDetails_t    //LPA packet details (for LPA plugins)
{
  char FieldDomain[33];       //field 'Domain'      in LPA packet details
  char FieldSource[128];      //field 'Source'      in LPA packet details
  char FieldDestination[128]; //field 'Destination' in LPA packet details
  char FieldMessage[64];      //field 'Message'     in LPA packet details
  char **FieldData;           //field at the bottom of LPA packet details
} LpaPacketDetails_t;
```

The members `FieldDomain`, `FieldSource`, `FieldDestination` and `FieldMessage` correspond to the fields 'Domain', 'Source', 'Destination' and 'Message' of the packet detail area. The member `FieldData` is an array of strings that represents the data listbox at the bottom of the packet detail area. The maximum number of lines in `FieldData` is `LPA_PDET_MAX_LINES`, the maximum length of one line is `LPA_PDET_MAX_CHARS`. If not all lines are used, the line after the last used line must be set to the null-string (`FieldData[Lastline+1][0]='\0'`). All values of the `LpaPacketDetails` structure can be changed within the `LpaPlgChangePacketDetails` function. If changes have been made, the function must return `TRUE`, otherwise it must return `FALSE`. Observe that since Plug-Ins are

executed in the same context as the LPA itself, a Plug-In can crash the LPA if it is not programmed correctly.

A sample implementation of an LPA Plug-In DLL is shown in the example 'LpaPlgT' which is located in the folder 'SOURCE\LpaPlgT' of your LPA installation directory. The file 'LpaPlgT.c' contains the source code of the DLL. The file 'LpaPFmt.h', where all needed structure types as well as constants are defined, is included in 'LpaPlgT.c'. The file 'LpaPlgT.def' is used to export the two DLL functions. A Visual C++ 7.1 solution file called 'LpaPlgT.sln' is also available. The following settings have been made in the Visual C++ Developer Studio: In [menu Project | Properties | C/C++ | Code Generation] the 'Struct Member Alignment' is set to 1 Byte and the 'Runtime Library' is set to 'Multi-threaded DLL'. In [menu Project | Properties | C/C++ | Advanced] the 'Calling Convention' is set to '__cdecl'.

All three settings are necessary for working correctly with the LPA Plug-In interface. A compiled version of the DLL is available in the folder 'SOURCE\LpaPlgT\Release' as well as in the folder 'PLUGIN'. It is called 'LpaPlgT.dll' and can be used with the LPA right away (see Section 5.11). If used it will change the display of all application messages with the message code 5, see Figure 48.

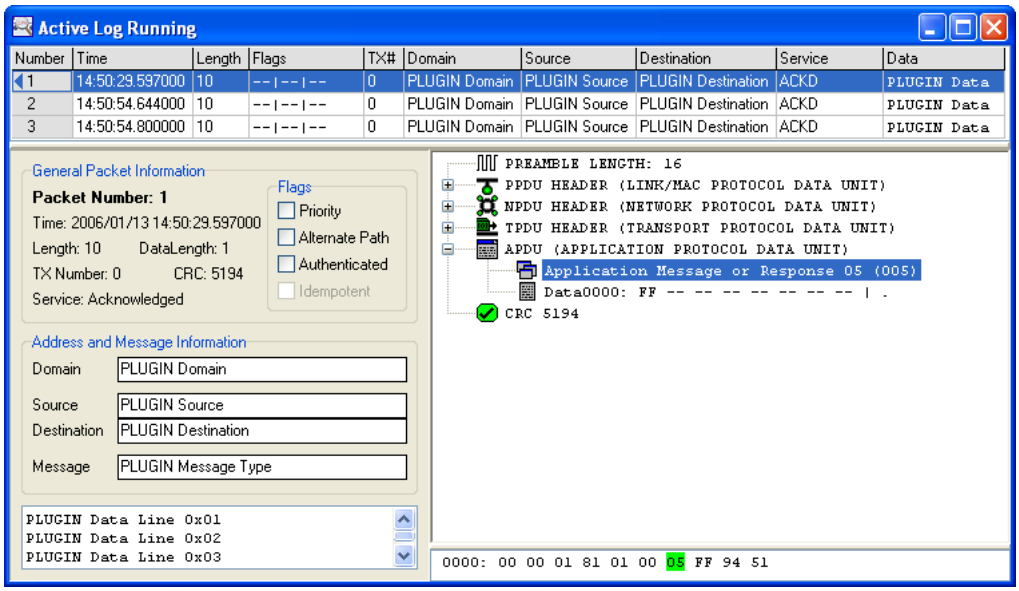

Active Log Running
Number Time Length Flags TX# Domain Source Destination Service Data
1 14:50:29.597000 10 --|--|-- 0 PLUGIN Domain PLUGIN Source PLUGIN Destination ACKD PLUGIN Data
2 14:50:54.644000 10 --|--|-- 0 PLUGIN Domain PLUGIN Source PLUGIN Destination ACKD PLUGIN Data
3 14:50:54.800000 10 --|--|-- 0 PLUGIN Domain PLUGIN Source PLUGIN Destination ACKD PLUGIN Data
General Packet Information
Packet Number: 1
Time: 2006/01/13 14:50:29.597000
Length: 10 DataLength: 1
TX Number: 0 CRC: 5194
Service: Acknowledged
Flags
Priority
Alternate Path
Authenticated
Idempotent
Address and Message Information
Domain PLUGIN Domain
Source PLUGIN Source
Destination PLUGIN Destination
Message PLUGIN Message Type
PLUGIN Data Line 0x01
PLUGIN Data Line 0x02
PLUGIN Data Line 0x03
PREAMBLE LENGTH: 16
PPDU HEADER (LINK/MAC PROTOCOL DATA UNIT)
NPDU HEADER (NETWORK PROTOCOL DATA UNIT)
TPDU HEADER (TRANSPORT PROTOCOL DATA UNIT)
APDU (APPLICATION PROTOCOL DATA UNIT)
Application Message or Response 05 (005)
Data0000: FF -- -- -- -- -- -- -- | .
CRC 5194
0000: 00 00 01 81 01 00 05 FF 94 51

Figure 48: **LPA Plug-In**

6.4 LPA Report DLLs

To create custom LPA report types (see Section 5.7), the LPA report DLL interface can be utilized. The function `LparGenerateReport` must be implemented in the custom DLL:

```
DWORD LparGenerateReport (
  LparGetUint_t *LparGetUint,   //function to get an unsigned integer value
  LparGetStr_t *LparGetStr,     //function to get a character array
  LparAddLine_t *LparAddLine    //function to add a new line to report
)
```

This function is called by the LPA whenever a report is requested by the user. The three parameters are callback function pointers the custom DLL must use to implement the report generation. The prototypes of these functions are defined in 'SOURCE\LpaRpt\LpaRpt.h':

```
typedef DWORD __cdecl LparGetUint_t(
  DWORD Type,                   //type of statistics value (general, etc.)
  DWORD ItemIdx,                //item index if not general type
  DWORD ValueIdx                //value index
);
```

The `LparGetUint` function is used to get a certain integer value from the LPA statistics of the current log. The parameter `Type` specifies which type of value is requested: `LPAR_GEN` specifies general statistics values, such as total packet count or number of bad packets. `LPAR_DOM`, `LPAR_SUB`, `LPAR_NOD`, `LPAR_GRP` specify values that are associated with a certain domain, subnet, node, or group. In this case, the parameter `ItemIdx` specifies the index of the domain, subnet, node, or group. Otherwise (`Type=LPAR_GEN`), `ItemIdx` must be set to 0. `ValueIdx` specifies the index of the requested integer value. The available value indices are defined and documented in 'SOURCE\LpaRpt\LpaRpt.h'.

```
typedef const char* __cdecl LparGetStr_t(
  DWORD Type,                   //type of statistics value (general, etc.)
  DWORD ItemIdx,                //item index if not general type
  DWORD ValueIdx                //value index
);
```

The `LparGetStr` function is used to get a certain string from the LPA statistics of the current log. The parameter `Type` specifies which type of string is requested: `LPAR_GEN` specifies general statistics string, such as LPA version string or log file name. `LPAR_DOM`, `LPAR_SUB`, `LPAR_NOD`, `LPAR_GRP` specify strings that are associated with a certain domain, subnet, node, or group. In this case, the parameter `ItemIdx` specifies the index of the domain, subnet, node, or group. Otherwise (`Type=LPAR_GEN`), `ItemIdx` must be set to 0. `ValueIdx` specifies the index of the requested string. The available string indices are defined and documented in 'SOURCE\LpaRpt\LpaRpt.h'.

```
typedef void __cdecl LparAddLine_t(
  LONG Mode,                    //line add mode (must be set to LPAR_MNORM)
  void *Line,                   //line to add (must point to character array)
  LONG InsNo                    //line number to insert (LPAR_END to append)
);
```

The `LparAddLine` function is used to add a line to the report. The parameter `Mode` must be set to `LPAR_MNORM`. The parameter `Line` must point to a string (character array) that contains the line to be added. The parameter `InsNo` specifies a line number, where the new line shall be inserted. If `InsNo` is set to `LPAR_END`, the line is appended at the end of the report.

The folder 'SOURCE\LpaRpt' in your LPA installation folder contains the full source code of the English and German LOYTEC Report DLLs. Both projects are integrated in the Visual C++ solution file 'LpaRpt.sln'. A translation to a different language can easily be performed by only translating one of the files 'LpaRptLocEng.h' or 'LpaRptLocGer.h'. Changes in the structure of the report file can be made in 'LpaRpt.c'. The finished DLL must then be named properly and copied to the 'RPTTYPE' folder. When starting the LPA, the DLL is automatically added to the available report types.

7 Revision History

Date	Version	Author	Description
11.05.2000	2.3	AB	Initial Version
22.01.2001	2.4	AB	New Features of LPA v2.4
11.12.2001	2.5	AB	New Features of LPA v2.5
23.07.2002	2.6	AB	New Features of LPA v2.6
02.06.2003	2.7	AB	Added Section 2.3 Network Interface and Transceiver Selection, LPA-IP Additions (LPA running on NIC852, see 2.3.2 and 2.3.3), Support of Multiplexed Network Interfaces (MNI Devices, see 2.3.5), Minor changes in other sections.
29.01.2004	2.8	AB	Numerous Changes in Chapter 2 Installation and Setup, Added Section 2.3.4 NIC-IP Devices.
23.02.2004	2.9	AB	Some minor changes
24.01.2005	2.11	AB	Additional Info in Network Interface Selection, see Figure 1, Figure 13, Improved documentation of Packet Storage Mode in Section 5.1, Chapter 6: All example projects available for Visual C++ 7.1.
24.02.2005	2.12	AB	LPA Server-only mode, see Section 2.7, extended APDU filtering, see Section 5.3.
04.04.2005	2.13	AB	Some minor changes
18.01.2006	3.0	AB	New Section 2.4 Command Line File Open, Section 4.3: Added transaction identification, Section 4.6: Added ‘Adjust Columns’ and Filtering / Conversion, Section 4.8: Added LPA 3.0 information in log files, Section 5.1: Added field ‘Trend Size’, Section 5.5: Added new error counters, New Section 5.6 Node Statistics, New Section 5.7 LPA Reports , New Section 5.8 Statistics Trends, New Section 6.4 LPA Report DLLs.
07.03.2007	3.1	AB	Some minor changes and correction of typos.
24.07.2007	3.2	AB	Up to 512 L-IPs can now be assigned, see Section 2.3.3, Up to 512 NIC-IPs can now be assigned, see Section 2.3.4.
14.01.2008	3.3	AB	Changed the standard term ‘EIA’ into ‘CEA’. Generic Remote-LPA Support (not restricted to L-IPs), see Section 2.3.3. NIC-IP configuration removed, see Section 2.3.4.

Abbreviations

ACK	. . .	Acknowledgement
ACKD	. . .	Acknowledged Message
APDU	. . .	Application Protocol Data Unit
AuthPDU	. . .	Authentication Protocol Data Unit
CNIP	. . .	Control Network over IP
CRC	. . .	Cyclic Redundancy Check
CSV	. . .	Comma Separated Value
DLL	. . .	Dynamic Link Library
LAN	. . .	Local Area Network
LPA	. . .	LOYTEC Protocol Analyzer
Mbps	. . .	Megabits per second
MDI	. . .	Multiple Document Interface
MNI	. . .	Multiplexed Network Interface
NID	. . .	Unique Node ID
NPDU	. . .	Network Protocol Data Unit
NV	. . .	Network Variable
PDU	. . .	Protocol Data Unit
SNVT	. . .	Standard Network Variable Type
SPDU	. . .	Session Protocol Data Unit
TPDU	. . .	Transport Protocol Data Unit
WAN	. . .	Wide Area Network

List of Figures

Figure 1: **Network Interface Selection** 7

Figure 2: **NIC709 Setup** 8

Figure 3: **NIC709 Transceiver Selection** 8

Figure 4: **LPA-IP running on NIC852** 9

Figure 5: **CEA852 Packet Logging** 9

Figure 6: **NIC852 Transceiver Selection** 10

Figure 7: **Remote LPA running on L-IP** 11

Figure 8: **Remote LPA Assignment** 11

Figure 9: **Assign/Add Remote LPA Device** 12

Figure 10**: Add CEA852 Channel** 12

Figure 11: **Transceiver Display for Remote-LPA Devices** 13

Figure 12: **Multiplexed Network Interfaces** 13

Figure 13: **Expert Mode for Network Interface Selection** 14

Figure 14: **LPA Server Systray Icon** 16

Figure 15: **Systray Icon Menu** 16

Figure 16: **Active Log Window** 17

Figure 17: **Incoming Packets** 17

Figure 18: **Packet Details** 18

Figure 19: **Converted Packets** 18

Figure 20: **Packet Statistics Window** 19

Figure 21: **End of Demonstration Log** 19

Figure 22: **Log Window of Packet Log File** 20

Figure 23: **Main Window of the LPA** 21

Figure 24: **Button and Corresponding Menu Item** 22

Figure 25: **Log Window** 24

Figure 26: **Network Management and Diagnostic Messages** 25

Figure 27: **SNVT Messages** 25

Figure 28: **Status Bar** 26

Figure 29: **Find Packet** 27

Figure 30: **Go To Packet** 27

Figure 31: **Popup Menu (View Menu)** 28

Figure 32: **Print Log** 30

Figure 33: **Log Mode** 31

Figure 34: **Packet Converter** 33

Figure 35: **Node Editor** 34

Figure 36: **Packet Filter** 36

Figure 37: **Address and APDU Table** 37

Figure 38: **Address Editor** 37

Figure 39: **Display Options** 40

Figure 40: **Packet Statistics for Current Log Window and Active Log** 41

Figure 41: **Node Statistics** 43

Figure 42: **Popup Menu of Node Statistics** 45

Figure 43: **LPA Report** 46

Figure 44: **Statistics Trends** 47

Figure 45: **Packet Simulation** 48

Figure 46: **Packet Creation** 48

Figure 47: **LPA Settings** 50

Figure 48: **LPA Plug-In** 55

Index

A

acknowledged 44
active log 21
Address and APDU table 36
address editor 37
address format 40
adjust columns 28, 44
advanced features 31
alternate path 43
APDU 26, 36, 49
APDU entries 38
application messages 25
ASCII 25
AuthPDU 26
AuthPDU header 49

B

bad packets 41, 42, 49
bandwidth utilization 41
broadcast 25

C

capture filter 22, 35
CEA709 5
CEA852 ..... 5, 10
channel member 11
clear log 23
CNIP 5
collisions 42
command line parameter 15
context-sensitive 30
converter file 32
converter options 40
converter settings 51
corrupted packets 42
CRC 48
CRC-error 26
CSV file 30, 45, 48, 52

D

data format 40
data mask 39
default directories 51
default files 51
demonstration file 19
destination address 24, 38
direction 34, 39
display filter 23, 35, 45
display options 23, 39
DLL 53, 55, 56
domain 24, 33, 37, 43
domain ID 33, 34, 37
domain index 35
domain tables 34

E

error counters 42
event-recording 50
exit LPA 20
export 48

export log 30
export settings 52
export table 45
external applications 51, 53

F

filter file 35
filter section 36
find packet 23, 27
flags 24
font size 30

G

go to packet 23, 27, 48
good packets 36, 41, 49
group 25, 33, 34, 35, 38, 43
group ID 33

H

help system 30
hidden packets 28, 41
hide columns 28

I

input network variable 34
installation 6
interface settings 7, 22
interrupted packets 42
IP-852 9

L

LAN 10
landscape format 30
layer 2 49
layer 3 49
layer 4 49
layer 5 49
LConfig 6
line number 24, 27
L-IP 10
log from network 23, 29
log mode 22
log mode settings 31
log statistics 41
log status 26
log window 24
lost packets 26, 42
LOYTEC Configuration tool 6
LOYTEC Protocol Analyzer 5
LOYTEC Software CD 6
LPA 5
LPA Client 53
LPA configuration 15
LPA menus 21
LPA Plug-In 42, 51, 55
LPA Server 42, 51, 53
LPA Server-only mode 15
LPA settings 50
LPA Software 6
LPAConv 51
LPA-IP 5, 8, 10
LPA-IP-SW 5
LPA-SW 5

M

main window 21

marked packets 28, 41
MD5 authentication 12
MDI 21
measurement system 51
menu item 21
merge converter files 32
message codes 25
message data 24
message type 42
missed preambles 42
MNI devices 13
Multiplexed Network Interfaces 13

N

negative entry 37
network addresses 32, 36
network diagnostic messages 25
network interface 5, 6, 22
network interface configuration 6
network management messages 25
network variables 34, 39
new log 22
NIC Software 6
NIC709 ..... 6, 7
NIC852 ..... 6, 8, 10
NIC-IP 13
NID 25, 34, 38
node 34, 43
node editor 34
node info 34
node name 34, 38
node number 25, 34, 35, 38
node statistics 43
NPDU 26
NPDU header 49

O

on-line 50
on-line mode 29, 32
open log 15, 22
output network variable 34

P

packet buffer 31
packet converter 23, 28, 32, 45
packet creation 49
packet details 25
packet filter 28, 35
packet length 24
packet log 21
packet log file 21, 29
packet recording file 31, 50, 52, 53
packet simulation 48
packet size 41
packet statistics 23, 41
packet storage mode 31
packet table 24
pass packets 37
pause log 18, 23
pause update 23
PDU format 41
PDU type 41
personal computer 5

Personal Firewall 6
popup menu..... 27, 45
positive entry..... 37
PPDU 26
PPDU header..... 49
print log..... 30
protocol details..... 26
protocol error 25, 42, 48

R

receiver..... 43
registration 6
reject packets..... 37
Remote Device Discovery 10
Remote LPA..... 5, 10
Remote LPA Assignment..... 10
report..... 46, 56
restart log 19

S

save log 22
selector 34, 39
sender 43
service 24, 41
shortcut key..... 21, 29
show columns 28
silent node 43
SNVT 25, 35
sort 43
source address 24, 38
SPDU 26
SPDU header 49
split PRC files 50
start log 17
status bar 26
stop log..... 19, 23
subnet..... 25, 33, 34, 35, 38, 43
subnet ID..... 33
symbolic name 32
system performance 48

T

time stamp..... 10, 13, 14, 24, 50, 52
time stamp format 40
time stamp mode 40
tool bar 22
TPDU 26
TPDU header 49
trace mode..... 50
transaction identification..... 25
transaction number..... 24
transceiver..... 26
transceiver selection..... 7
trend 31, 47
trigger..... 22, 35

U

USB key..... 8

W

WAN..... 10